

Policies

EXECUTIVE SUMMARY

POLICY NUMBER AND TITLE: Policy 2460-Safety and Acceptable Use of the Internet by Students and Educators

BACKGROUND:

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

CONTENTS:

Policy 2460 includes regulations for the safety and use of the Internet. It addresses acceptable use, privileges, accountability and responsibility, web publishing, network etiquette, reliability, security, safety, and vandalism.

PURPOSE:

Policy 2460 has been revised (1) to include the new federal regulations regarding issues of child safety and acceptable use of the Internet and (2) to be in compliance with Universal Service Fund for Schools and Libraries (E-rate) guidelines.

The policy was placed on public comment until July 20, 2001, and three people responded. Clarification and technical changes were made to the policy based on the comments received. The comment log is attached.

TITLE 126

LEGISLATIVE RULE

BOARD OF EDUCATION

SERIES 41

SAFETY AND ACCEPTABLE USE OF THE INTERNET

BY STUDENTS AND EDUCATORS (2460)

§126-41-1. General.

1.1. Scope - This legislative rule establishes criteria for the safety and acceptable use of the Internet by students, educators, school personnel, and the West Virginia Department of Education employees.

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

1.3. Filing Date - August 10, 2001

1.4. Effective Date - September 9, 2001

§126-41-2. Scope.

2.1. The Internet is an electronic highway connecting millions of computers all over the world and millions of individual subscribers. Access to the Internet will provide students and educators with:

2.1.1. electronic mail communication;

2.1.2. information and news services;

2.1.3. public domain and software of all types;

2.1.4. discussion groups on a variety of subjects;

2.1.5. connections to many libraries, companies, agencies, and businesses;

2.1.6 virtual courses and educational resources;

2.1.7 online staff development;

2.1.8 electronic educational tools and e-learning platforms.

2.2. 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 ensure that access to telecommunication networks, computers and the Internet provided by the school, county, RESA and state educational systems is not abused.

§126-41-3. Use.

3.1. Acceptable Use.

3.1.1. The purpose of the National Science Foundation Network (NSFNet), which was the original Internet backbone network, was to support research and education in and among academic institutions in the U.S. by providing access to unique resources and the opportunity for collaborative work. Access to the Internet for West Virginia schools is provided in the spirit of that original intent for academic achievement. The use of the Internet must be in support of education and consistent with the educational objectives of the West Virginia Board of Education (WVBE). Use of other networks or computing resources must comply with the rules appropriate for that network. Users must also be in compliance with the rules and regulations of the West Virginia Network for Educational Telecomputing (WVNET) specifically the: "WVNET Security Policy and Procedure."

3.1.2. 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. Use for commercial activities by for-profit institutions is generally not acceptable. Use for product advertisement or political lobbying is also prohibited. Illegal activities and privacy and safety violations of the Children's Online Privacy Protection Act (COPPA) and the Children's Internet Protection Act (CIPA) are strictly prohibited.

3.2. Privileges.

3.2.1. The use of the Internet as part of an educational program is a privilege, not a right, and inappropriate or unauthorized use or safety violations could result in revocation or suspension of that privilege. Each student who will access the Internet will be provided acceptable use training and shall have an acceptable use form, signed by a parent or legal guardian, on file. No temporary accounts will be issued, nor will a student use an Internet account not specifically created for him or her. Based upon the acceptable use and safety guidelines outlined in this document, the West Virginia Department of Education (WVDE) and the WVNET system administrators will determine what is appropriate use, and their decision is final. Also, the system administrator and/or local teachers may deny user access at any time. Additionally, the State of West Virginia may pursue legal action to recover damages as a result of inappropriate use or safety violations of the network.

3.2.2. The WVDE's administrative information systems (WVEIS) are to be used exclusively for the business of the organization. All information system messages are records of the WVDE. The WVDE reserves the right to access and disclose all messages sent over its information systems for any purposes. For reasons of privacy, employees may not attempt to gain access to another employee's personal file of messages 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.

3.3. Accountability and Responsibility.

3.3.1. The use of telecommunications and/or access to the Internet is an extension of the educator's responsibility in his/her classroom. Therefore, it is the educator's responsibility to ensure classroom activities that utilize Internet-related technologies focus on appropriate and specific learning goals and objectives. All student use of Internet-related applications must be authorized by the educator. Specific examples of unauthorized use include, but are not limited to:

- a. Executing non-educational gaming.
- b. Creating, storing, sending, or viewing pornographic material.
- c. Downloading, uploading and/or executing viruses.
- d. Using e-mail user IDs other than one's own ID.
- e. Misrepresenting an individual's identity or source of communication or data.
- f. Illegally accessing or attempting to access another person's data or personal system files.
- g. Corrupting, destroying, deleting, or manipulating system data with malicious intent.
- h. Requesting that inappropriate material be transferred.
- i. Violating safety and/or security measures when using e-mail, chat rooms, and other forms of direct electronic communications.
- j. "Hacking" or any other unlawful online activities.
- k. Disclosing, using, or disseminating personal information regarding minors.

3.3.2. The use of telecommunications and/or access to the Internet is an extension of the students' responsibility in the classroom. Educators are encouraged to define a student code of conduct or set of responsibilities for the safety and acceptable use of telecommunications in the classroom. The use and administration of a network server for Internet connection within a county or school is the responsibility of the 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 educator/administrator at that location. At no point should a student be given administrative responsibilities for a server with a wide-area network or Internet connection.

3.3.3. The WVDE and WVNET can only monitor those e-mail accounts issued to the "access.k12.wv.us" server, which is administered by WVDE and WVNET. The responsibility for any "non-access.k12.wv.us" e-mail accounts lies with the administrator(s) and/or educator(s) identified as responsible for those students using alternative e-mail accounts or the administrator(s) and/or educator(s) identified as responsible for the e-mail server being used.

3.3.4. All access to "Dial-up" 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. Dial-up access of any kind is only to be used when specific educational goals have been identified and is not to be in direct competition with local Internet service providers. Additionally, all "dial-up" servers must not conflict with federal, state and local guidelines for appropriate Internet access.

3.3.5. Those 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.

3.4. Web Publishing.

3.4.1. 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, and student protection. In addressing these issues, the WVDE recommends that each county and/or school adopt local policies that are consistent with the following "Web Publishing Guidelines".

3.4.2. The "official" web site may be designated by the school through the faculty senate, the school improvement council, the school technology committee, or the administration.

3.4.3. Parental 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.

3.4.4. 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.

3.4.5. Content of a web site:

a. Content should be appropriate, in good taste, and not harmful to any individual or group.

b. Text should be grammatically correct, accurately spelled, and have a pleasing appearance.

c. Student pictures and names can be published on the school/county web site at the discretion of the school/county. 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.

d. Pages should comply with WVBE policies and regulations.

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

f. Information on a page should remain current and be accurate.

g. Business/commercial links or the acknowledgment of a business on a school/county web site should be restricted 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.

h. All content must comply with copyright, intellectual property, state, federal (specifically the Children's Online Privacy Protection Act (COPPA) and the Children's Internet Protection Act (CIPA)) and international law.

i. Published copyrighted materials must include the permission granted statement (who, time period, etc.).

j. Documents should be available to validate published information.

3.4.6. Navigation/Organization of a web site:

a. Navigation through the site should be easy and user friendly.

b. Text-only browsers and technical specifications necessary for handicapped accessibility need to be considered when creating a web site.

c. Links should be checked periodically for "dead links."

d. Bandwidth requirements should be considered when designing a home page. Use limited graphics, smaller graphics, few animations, few sounds, and other scripting means to lower the bandwidth requirements in accessing the home page.

3.4.7. Style/Markup of web pages:

a. Every web page should have a title and top level heading that are the same and reference the theme of the home page.

b. Text highlighting (italics, bold, underline) should be used sparingly.

c. Large documents should be divided logically.

d. Thumbnail images should be used to link to larger images where possible.

e. Every graphic should have an associated and meaningful (ALT) text.

f. Proprietary markup should be avoided. Write to the current HTML standard.

3.5. Domain Name Server Application.

3.5.1. If a school or county is running or wishes to run a network server, that school/county must request an application from the WVDE Office of Technology to be granted an appropriate domain name. As part of the application process the school/county is required to have local guidelines for web publishing as part of their acceptable use policy. A copy of that document must be on file with the WVDE.

3.6. Network Etiquette.

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

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

b. Use appropriate language. Do not swear, use vulgarities or any other inappropriate language.

c. Do not reveal the personal home address or phone number of students or colleagues. -- Note that electronic mail (e-mail) is not guaranteed to be private. Messages related to or in support of illegal activities may be reported to the authorities.

d. 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).

e. Keep files (old e-mail messages) stored on the server to a minimum.

f. If account is to be unused for an extended period of time, be sure to unsubscribe to listservs.

3.7. Reliability.

3.7.1. The WVDE and WVNET make no warranties of any kind, whether expressed or implied, for the service being provided. The WVDE and WVNET 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 and WVNET are not responsible for the accuracy and quality of information obtained through the system.

3.8. Security.

3.8.1. Users who identify a security problem on the system must notify a system administrator. Users must not demonstrate the problem to other users. Users must not use another individual's account or give their passwords to others. Attempts to log into the system as a system administrator will result in revocation of user privileges. Any user identified as a security risk or having a history of problems with other computer systems may be denied access.

3.8.2. 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.

3.9. Vandalism.

3.9.1. Vandalism will result in revocation of user privileges. Vandalism is defined as any attempt to harm or destroy data of another user or any connections that are part of the Internet. This includes, but is not limited to, uploading, downloading or creating computer viruses.

3.10. Safety.

3.10.1. Safety measures must be enforced to carry out policies at the state, county, and school to implement the intent of CIPA, COPPA and E-rate guidelines.

3.10.2. The WVDE, county school systems and schools, in partnership with WVNET and other appropriate state agencies, will organize technical protection measures to guard against visual depictions that are (1) obscene; (2) child pornography; or (3) harmful to minors or other material deemed locally to be "inappropriate for minors."

3.10.3. The WVDE and WVNET operate the statewide infrastructure to provide Internet access for all Pre-K-12 public schools. In accordance with state purchasing guidelines, filtering will be installed at the state 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.

3.10.4. The county school systems and/or schools may also add other electronic filters at the local levels.

3.10.5. Schools must enforce the use of the filtering or electronic technical protection measure during any use of the computers to access the Internet.

3.10.6. Safety includes monitoring the online activities of minors through the filtering of Internet access to the World Wide Web.

§126-41-4. Implementation.

4.1. County Boards of Education.

4.1.1. County boards of education will ensure implementation of this policy in a method that promotes proper use of the Internet. County boards should consider adopting their own policies regarding telecommunications networks.

4.2. West Virginia Department of Education (WVDE).

4.2.1. The WVDE shall provide technical assistance to support county school systems and schools in implementing this policy. The WVDE will also provide assistance to Regional Education Service Agencies (RESAs), counties, and schools in developing local use policies.

West Virginia Department of Education
1900 Kanawha Boulevard East, Charleston, WV 25305
[\(Staff Phone and Email by Name\)](#) [\(School Directory\)](#)

Topics: [A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [J](#) [K](#) [L](#) [M](#) [N](#) [O](#) [P](#) [Q](#) [R](#) [S](#) [T](#) [U](#) [V](#) [W](#) [X](#) [Y](#) [Z](#)

For suggestions, questions, problems contact the [webmaster](#)
Please read our [disclaimers](#)

[State Board](#) | [Department](#) | [Teachers](#) | [Parents](#) | [Students](#) | [Community](#) | [Data](#)