

1.0 **PURPOSE:**

Advances in telecommunications and other related technologies have fundamentally altered the ways in which information is accessed, communicated, and transferred in our society. Such changes are driving the need for educators to adapt their means and methods of instruction, and the way they approach student learning, to harness and utilize the vast, diverse, and unique resources available on the Internet. The Board of Education is pleased to provide Internet service to its staff and students. The County's Internet system has a limited educational purpose. The County's internet system has not been established as a public access service or a public forum. The Board has the right to place restrictions on its use to assure that use of the County's Internet system is in accord with its limited educational purpose. Staff and student use of the County's computers, network, and Internet services ("network") will be governed by this policy and the related administrative guidelines, and West Virginia State Board of Education Policy 2460. The use of the Internet as part of an educational program is a privilege, not a right, and inappropriate or unauthorized use of safety violations may result in revocation or suspension of the privilege. The due process rights of all users will be respected in the event there is a suspicion of inappropriate use of the network. Users have no right or expectation to privacy when using the network (including, but not limited to, privacy in the content of this personal files, e-mails, and records of their online activity while on the network).

2.0 **ADMINISTRATION:**

The Board supports our one-one initiative for staff and students in order to promote educational excellence in our schools by providing them with the opportunity to develop the resource sharing, innovation, and communication skills and tools which will be essential to life and work in the 21st century. Technology must be interwoven with educational improvements and reform to accomplish educational goals, increase student achievement and provide increased opportunities for lifelong learning. The Board encourages the staff and students to develop the appropriate skills necessary to effectively access, analyze, evaluate, and utilize these resources in enriching educational activities.

2.1 The use of the electronic resources, technologies, and the Internet must be in support of education and consistent with the educational objectives and priorities of the West Virginia Board of Education (WVBE). Use of other networks and computing resources must comply with the rules appropriate for that network and copyright compliance. Users must also be in compliance with the rules and regulations of the network provider(s) serving the County and its schools.

2.2 The Internet is a global information and communication network that provides an incredible opportunity to bring previously unimaginable education and information resources to our students. The Internet connects computer and users in the County with computers and users worldwide. Through the Internet, students and staff can access up to date, highly relevant information that will enhance their learning and the education process. Further, the Internet provides students and staff with the opportunity to communicate with other people from throughout the world. Access to such an incredible quantity of information and resources brings with it, however, certain unique challenges and responsibilities.

- 2.3 First, and foremost, the Board may not be able to technologically limit access to services through the Board's Internet connection to only those that have been authorized for the purpose of instruction, study and research related to the curriculum. Unlike in the past when educators and community members had the opportunity to review and screen materials prior to student use to assess their appropriateness for supporting and enriching the curriculum according to adopted guidelines and reasonable selection criteria (taking into account the varied instructional needs, learning styles, abilities, and developmental levels of the students who would be exposed instructional needs, learning styles, abilities, and developmental levels of the students who would be exposed to them), access to the Internet, because it serves as a gateway to any publicly available file server in the world, will open classrooms and students to electronic information resources which have not been screened by educators for use by students of various ages.
- 2.4 The West Virginia Department of Education (WVDE), approved service provider, and other State agencies operate the statewide infrastructure to provide Internet access for all Pre-k-12 public schools. Pursuant to Federal law, the State has implemented technology protection measures, which protect against (e.g., filter or block) access to visual displays/depictions/materials that are obscene, constitute child pornography, and/or are harmful to minors, as defined by the Children's Internet Protection Act. Filtering will be installed at the State level at the two (2) points of presence (POPs) for Internet access. This will provide filtering for all public schools in a cost effective manner and with efficient management and enable the County/schools to meet the Children's Internet Protection Act (CIPA) and E-Rate guideline requirements for filtering.

3.0 PROCEDURES:

The Board will use technical protection measures to guard against visual depictions that are obscene, child pornography and other materials that are harmful to minors.

- 3.1 The technology protection measures may not be disabled at any time that students may be using the network, if such disabling will cease to protect against access to materials that are prohibited under the Children's Internet Protection Act. Any staff member who attempts to disable the technology protection measures without express written consent of an appropriate administrator will be subject to disciplinary action, up to and including termination.
- 3.2 Staff members and students will participate in professional development programs, as appropriate, in accordance with the provisions of this policy. Training shall include:
- 3.2.1 The safety and security of students while using e-mail, chat rooms, social networking sites and other forms of direct electronic communications;
 - 3.2.2 The inherent danger of students disclosing personally identifiable information online;
 - 3.2.3 The consequences of unauthorized access (e.g., "hacking"), cyberbullying and other unlawful or inappropriate activities by students or staff online; and
 - 3.2.4 Unauthorized disclosure, use, and dissemination of personal information regarding minors.

Furthermore, staff members shall provide instruction for their students regarding the appropriate technology use and online safety and security as specified above and staff members will monitor students' online activities.

- 3.3 Monitoring may include, but is not necessarily limited to, visual observations of online activities during class sessions; or use of specific monitoring tools to review browser history and network, server, and computer logs.
The disclosure of personally identifiable information about students online is prohibited.
- 3.4 Building principals are responsible for providing training so that Internet users under their supervision are knowledgeable about this policy and its accompanying guidelines. The Board expects that staff members will provide guidance and instruction to students in the appropriate use of the Internet. Such training shall include, but not limited to, education concerning appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response. All users are required to sign a written agreement to abide by the terms and conditions of this policy and its accompanying guidelines.
- 3.5 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 of 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.
- 3.6 Staff members and students are responsible for the use of the Board's computers/ network and the Internet in a manner consistent with this policy and its related guidelines. Communications on the Internet are often public in nature. Staff members and students shall not access social media for personal use on the District's network, and shall access social media for educational use only after submitting a plan for that education use and securing the principal's approval of that plan in advance.
- 4.0 **General school rules** including the Employee and Student Code of Conduct for behavior and communication apply. The Board does not sanction any use of the Internet that is not authorized by or conducted strictly in compliance with this policy and its accompanying guidelines. Users who disregard this policy and its accompanying guidelines may have their use privileges suspended or revoked, and disciplinary action taken against them. Users granted access to the internet, through the Board's computers, assume personal responsibility and liability, both civil and criminal, for uses of the Internet not authorized by the policy and its accompanying guidelines.
- 4.1 The use and administration of network server for Internet connection within the County or schools 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 function 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.

- 4.2 The West Virginia Department of Education (WVDE) and approved service provider(s) can only monitor those e-mail accounts issued to the “k12.wv.us” server, which is administered by WVDE and approved providers. The responsibility for any “non-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.
- 4.3 All remote access to servers located at the 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 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 remotely accessed servers must not conflict with Federal, State, and local guidelines for appropriate Internet access.
- 4.4 Those server administrators or technical contacts requesting domain names for local servers must apply to the WVDE or the Wirt County Board of Education 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.

5.0 NETWORK SECURITY

The WVDE and the WCBOE 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, application, bandwidth utilization, document files, folders, electronic communication, e-mail, Internet access, and any and all information transmitted or received in connection with networks, e-mail use and web-based tools.

- 5.1 The WVDE’s administrative information system (WVEIS) is to be used exclusively for the business of the organization. All information system data are records of the organization. The WVDE has reserved 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).
- 5.2 For reasons of privacy, employees may not attempt to gain access to another employee’s personal file of messages in the WVDE’s or WCBOE’s information systems. However, the WVDE and WCBOE has reserved the right to enter an employee’s information system files whenever there is a business need to do so.
- 5.3 Based on the acceptable use and safety guidelines outlined in West Virginia State Board of Education Policy 2460, the State Superintendent, the WVDE and provider(s) system administrators and/or local teachers may deny user access at any time.

- 5.4 Downloading, copying, duplicating, and distributing software, music, sound files, movies, images, or other copyrighted material 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.
- 5.5 The Board designates the Superintendent as the administrators responsible for initiating, implementing, and enforcing this policy and its accompanying guidelines as they apply to the use of the Network and the Internet for instructional purposes.

6.0 SOCIAL MEDIA USE

- 6.1 An employee's personal or private use of social media, such as Facebook, Twitter, blogs, etc., may have unintended consequences. While the Board respects its employees' First Amendment Rights, those rights do not include permission to post inflammatory comments that could compromise the County's mission, undermine staff relationships, or cause a substantial disruption to the school environment. This warning includes staff members' online conduct that occurs off school property including from the employee's private computer. Posting to social media should be done in a manner sensitive to the staff member's professional responsibilities.
- 6.2 In addition, Federal and State confidentiality laws forbid schools and their employees from using or disclosing student education records without parental consent (see Policy [8330](#)). Education records include a wide variety of information; posting personally identifiable information about students is not permitted. Staff members who violate State and Federal confidentiality laws or privacy laws related to the disclosure of confidential student or employee information may be disciplined.

7.0 **SEVEREBILITY:** If any provision of this policy or application thereof to any person or circumstance is held invalid, such invalidity shall not affect the provisions of applications of this policy.

8.0 AUTHORIZATION:

West Virginia State Board of Education Policy [2460](#)
H.R. 4577, P.L. 106-554, Children's Internet Protection Act of 2000
47 U.S.C. 254(h), (1), Communications Act of 1934, as amended (2003)
20 U.S.C. 6801 et seq., Part F, Elementary and Secondary Education Act of 1965, as amended
18 U.S.C. 2256, 18 U.S.C. 1460, 18 U.S.C. 2246, 20 U.S.C. 6777, 9134 (2003), 76 F.R. 56295, 56303

Review Schedule:

This policy shall be reviewed in accordance with the policy review schedule published by the Superintendent.

Replaces: Network and Internet Acceptable Use for Students form in I – Instruction section of the policy manual, June 28, 2012. Student and Staff forms are available on WCBOE website.