7540.04 - STAFF TECHNOLOGY ACCEPTABLE USE AND SAFETY

Technology has fundamentally altered the ways in which information is accessed, communicated, and transferred in society. As a result, educators are continually adapting their means and methods of instruction, and the way they approach student learning, to incorporate the vast, diverse, and unique resources available through the Internet. The Board of Education provides Technology and Information Resources (as defined by Bylaw 0100) to support the educational and professional needs of its staff and students. The Board provides staff with access to the Internet for limited educational purposes only and utilizes online educational services/apps to enhance the instruction delivered to its students and to facilitate the staff's work. The District's computer network and Internet system do serve as a public access service or a public forum, and the Board imposes reasonable restrictions on its use consistent with its limited educational purpose.

The Board regulates the use of District Technology and Information Resources by principles consistent with applicable local, State, and Federal laws, and the District's educational mission. This policy and its related policy and administrative guidelines, policy 7544 and AG 7544, and any applicable employment contracts govern the staffs' use of the District's Technology and Information Resources and staff's personal communication devices when they are connected to the District's computer network, Internet connection and/or online educational services/apps, or when used while the staff member is on Board-owned property or at a Board-sponsored activity (see Policy 7530.02).

Users are required to refrain from actions that are illegal (such as libel, slander, vandalism, harassment, theft, plagiarism, inappropriate access, and the like) or unkind (such as personal attacks, invasion of privacy, injurious comment, and the like). Because its Technology Resources are not unlimited, the Board has also instituted restrictions aimed at preserving these resources, such as placing limits on use of bandwidth, storage space, and printers.

Users have no right or expectation to privacy when using District Technology and Information Resources (including, but not limited to, privacy in the content of their personal files, e-mails, and records of their online activity when using the District's computer network and/or Internet connection).

Staff members are expected to utilize District Technology and Information Resources to promote educational excellence in our schools by providing students with the opportunity to develop the resource sharing, innovation, and communication skills and tools that are essential to life and work. The Board encourages the staff to develop the appropriate skills necessary to effectively access, analyze, evaluate, and utilize these resources in enriching educational activities. The instructional use of the Internet and online educational services will be guided by Board Policy **2520** - Selection of Instructional Materials and Equipment.

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 or 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.

The Internet is a global information and communication network that brings incredible education and information resources to our students. The Internet connects computers and users in the District with computers and users worldwide. Through the Internet, students and staff can access relevant information that will enhance their learning and the education process. Further, District Technology Resources provide 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.

The Board may not be able to technologically limit access to services through its Technology Resources to only those services and resources 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 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 to them), access to the Internet, because it serves as a gateway to any publicly available file server in the world, opens classrooms and students to electronic information resources that may not have been screened by educators for use by students of various ages.

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, that 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. Electronic filtering will be installed by WVDE 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. This service enables the County/schools to meet the Children's Internet Protection Act (CIPA) and E-Rate guideline requirements for filtering.

The Board shall add other electronic filters at the school level.

With approval of the Board, schools may add other electronic filters at the local level.

The Board will use technical protection measures to protect against (i.e., filter or block) access to other material considered inappropriate for students to access. The Board also utilizes software and/or hardware to monitor online activity of staff members to restrict access to child pornography and other material that is obscene, objectionable, inappropriate and/or harmful to minors.

The technology protection measures may not be disabled at any time that students may be using the District Technology Resources, 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.

The Superintendent or Director of Technology may temporarily or permanently unblock access to websites or online educational services/apps containing appropriate material, if access to such sites has been inappropriately blocked by the technology protection measures. The determination of whether material is appropriate or inappropriate shall be based on the content of the material and the intended use of the material, not on the protection actions of the technology protection measures. The Superintendent or Director of Technology also may disable the technology protection measures to enable access for bona-fide research or other lawful purposes.

Staff members will participate in professional development programs in accordance with the provisions of law and this policy. Training shall include:

A. the safety and security of students while using e-mail, chat rooms, social media, and other forms of direct electronic communications;

B. the inherent danger of students disclosing personally identifiable information online;

C. the consequences of unauthorized access (e.g., "hacking", "harvesting", "digital piracy", "data mining", etc.), cyberbullying and other unlawful or inappropriate activities by students or staff online; and

D. unauthorized disclosure, use, and dissemination of personally identifiable 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 while at school.

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.

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 on the appropriate use of the District Technology Resources. Such training shall include, but not be limited to, education concerning appropriate online behavior, including interacting with other individuals on social media, including in chat rooms and cyberbullying awareness and response. All users of District Technology Resources are required to sign a written agreement to abide by the terms and conditions of this policy and its accompanying guidelines.

Staff will be assigned a school email address that they are required to utilize for all school-related electronic communications, including those to students, parents and other constituents, fellow staff members, and vendors or individuals seeking to do business with the district.

With prior approval from the Superintendent or Director of Technology, staff may direct students who have been issued school-assigned e-mail accounts to use those accounts when signing-up/registering for access to various online educational services, including mobile applications/apps that will be utilized by the students for educational purposes under the teacher's supervision.

Staff members are responsible for good behavior when using District Technology and Information Resources – i.e., behavior comparable to that expected when they are in classrooms, school hallways, and other school premises and school-sponsored events. Communications on the Internet are often public in nature. The Board does not approve any use of its Technology and Information Resources that is not authorized by or conducted strictly in compliance with this policy and its accompanying guidelines s and policy 7544 and its accompanying guideline.

Staff members may only use District Technology Resources to access or use social media if it is done for educational or business-related purposes.

Staff members use of District technology resources to access or use social media is to be consistent with policy 7544 and its accompanying guideline. An employee's personal or private use of social media 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 District'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. Postings to social media should be done in a manner sensitive to the staff member's professional responsibilities and in compliance with State board policy 5902. Inappropriate online behavior may be cause for discipline pursuant to the provisions of West Virginia Code 18A-2-8.

General school rules for behavior and communication apply. Users who disregard this policy and its accompanying guidelines may have their use privileges suspended or revoked, and disciplinary action taken against them. Users are personally responsible and liable, both civilly and criminally, for uses of District Technology and Information Resources that are not authorized by this policy and its accompanying guidelines.

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 "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.

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.

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).

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 has reserved the right to enter an employee's information system files whenever there is a business need to do so.

Based on the acceptable use and safety guidelines outlined in WVBE policy 2460, the State Superintendent, the WVDE and provider(s) system administrators will determine what appropriate use is, and their decision is final. Also, the system administrator and/or local teachers may deny user access at any time.

The Board designates the Superintendent and Director of Technology as the administrators responsible for initiating, implementing, and enforcing this policy and its accompanying guidelines as they apply to staff members' use of District Technology and Information Resources.

West Virginia State Board of Education policy 2460 – Educational Purpose and Acceptable Use of Electronic Resources, Technologies and the Internet
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 (2003)
18 U.S.C. 1460
18 U.S.C. 2246
18 U.S.C. 2256
20 U.S.C. 6777, 9134 (2003)
47 C.F.R. 54.500 - 54.523

Adopted 6/18/12
Revised 9/1/15
Revised 12/6/16

STAFF NETWORK AND INTERNET ACCEPTABLE USE AND SAFETY

ACCEPTABLE USE POLICY FORM

As a user of the Randolph County Schools computer network, I have read and agree to comply with the Acceptable Use Policy (AUP). Should I commit any violation, my access privileges may be temporarily or permanently revoked and disciplinary action may be taken, up to and including suspension/termination. I understand that commission of any crime via Internet falls under State and Federal authority.

Print Name _____

Signature _____

Date _____

West Virginia State Board of Education policy 2460 – Educational Purpose and Acceptable Use of Electronic Resources, Technologies and the Internet
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 (2003)
18 U.S.C. 1460
18 U.S.C. 2246
18 U.S.C. 2256
20 U.S.C. 6777, 9134 (2003)
47 C.F.R. 54.500 - 54.523