ROANE COUNTY SCHOOLS

Policy ~~7540.04~~ 590 – ~~Staff Technology~~ Acceptable Use of Technology by Staff ~~and Safety~~

Revised policy and repeal of Policy 7540.05 (District-Issued Staff E-mail Account) effective upon passage

1st reading July 11, 2019

2nd reading

3rd reading

Statutory authority West Virginia Board of Education Policy 2460

Administrative Guidelines
(none)

~~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.

As West Virginia Board of Education Policy 2460 defines the acceptable use of technology for all students, staff, and visitors in West Virginia's K12 computer network and school facilities, the Board adopts this policy and incorporates it by reference here. The following provisions are intended to extend to local operation and in no way contradict or supplant WVBE Policy 2460.

The ~~District's~~ County's computer network and Internet system do not 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 administrative guidelines and any applicable employment contracts and collective bargaining agreements~~ governs ~~the~~ staffs' use of the ~~District's~~ County's technology and information resources and staff's personal communication devices when they are connected to the ~~District's~~ County'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)~~. For the purposes of this policy, staff shall include all professional and service personnel, those employed on extracurricular assignments, and Board members when acting in their official capacities.

~~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 County 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 both life and work. The Board encourages the faculty 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 State Board of Education. 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.~~

~~First,~~ The Board may not be able to technologically limit access~~, 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 State-wide 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 the 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~~ may add other electronic filters at the county or school 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 Technology Director~~ may ~~temporarily or permanently unblock~~ authorize temporary or permanent 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 Technology Director~~ also may ~~disable~~

authorize temporary disabling of 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 use of technology 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 in 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 e-mail address that they are required to utilize for all school-related electronic communications, including those to students, parents, and other staff members.~~

With prior approval from the Superintendent ~~or Technology Director~~, 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.~~

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

~~General school rules for behavior and communication apply.~~

~~Users~~ Staff who ~~disregard~~ are found to have violated this policy ~~and its accompanying guidelines~~ may have their use privileges suspended or revoked, and disciplinary action taken against them. ~~Users~~ Staff are personally responsible and liable, both civilly and criminally, for uses of ~~District~~ County 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 "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.~~

~~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 West Virginia State Board of Education policy 2460, the State Superintendent, the WVDE and provider(s) 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.~~

~~The Board designates the Superintendent and Technology Director 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.~~

Social Media Use

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.

Use of social media by staff using County technology resources shall be limited to educational purposes and those purposes which advance Board's interests.

~~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.~~

~~Staff members retain rights of communication for collective bargaining purposes and union organizational activities.~~

~~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 9/16/08~~
~~Revised 6/28/12~~
~~Revised 11/19/15~~
~~Revised 9/22/16~~

District-Issued Staff E-Mail Account
~~Staff~~

~~The Board of Education is committed to the effective use of electronic mail ("e-mail") by all District staff and Board members in the conduct of their official duties. This policy and any corresponding guidelines are intended to establish a framework for the proper use of e-mail for conducting official business and communicating with colleagues, students, parents and community members.~~

~~When available, The District's e-mail system~~ E-mail accounts issued to staff by the West Virginia Department of Education must be used by ~~employees~~ staff for any official ~~District~~ County e-mail communications. Personal e-mail accounts on providers other than the ~~District's~~ WVDE's e-mail system may be blocked at any time if concerns for network security, spam, or virus protection arise. ~~District~~ Staff are expected to exercise reasonable judgment and prudence and take appropriate precautions to prevent viruses from entering the ~~District's~~ County's network when opening or forwarding any e-mails or attachments to e-mails that originate from unknown sources.

~~District~~ Staff shall not send or forward mass e-mails, even if the e-mails concern ~~District~~ Board business~~, without prior approval of the Technology Director~~.

~~District~~ Staff may join list servs or other e-mail services (e.g. RSS feeds) that pertain to their responsibilities in the ~~District~~ County, provided these list servs or other e-mail services do not ~~exceed the staff member's e-mail storage allotment~~ become excessive. ~~If a staff member is unsure whether s/he has adequate storage or should subscribe to a list serv or RSS feed, s/he should discuss the issue with his/her building principal or the District's IT staff. The Technology Director is authorized to block~~ E-mail from list servs or e-mail services may be blocked if the e-mails received by ~~the~~ staff ~~member(s)~~ become excessive.

Staff ~~members~~ are encouraged to ~~keep their inbox and folders organized by regularly reviewing e-mail messages,~~ appropriately ~~saving~~ save e-mails that constitute a public record or student record and e-mails that are subject to a litigation hold ~~(see Policy 8315 - Information Management), and purging all other e-mails that have been read. If the staff member is concerned that his/her e-mail storage allotment is not sufficient, s/he should contact the District's IT staff.~~

Public Records

The ~~District~~ Board complies with all Federal and State laws pertaining to electronic mail. Accordingly, e-mails written by or sent to ~~District~~ staff and Board members may be public records if their content concerns ~~District~~ Board business, or education records if their content includes personally identifiable, non-directory information about a student. E-mails that are public records are subject to retention and disclosure, upon request~~, in accordance with Policy 8310 – Public Records~~. E-mails that are student records must be maintained ~~pursuant to Policy 8330 – Student Records~~. Finally, e-mails may constitute electronically stored information ("ESI") that may be subject to a litigation hold ~~pursuant to Policy 8315 – Information Management~~.

~~State and Federal law exempt certain documents and information within documents from disclosure, no matter what their form. Therefore, certain e-mails may be exempt from disclosure or it may be necessary to redact certain content in the e-mails before the e-mails are released pursuant to a public records request, the request of a parent or eligible student to review education records, or a duly served discovery request involving ESI.~~

E-mails written by or sent to ~~District~~ staff and Board members by means of their private e-mail account may be public records if the content of the e-mails concerns ~~District~~ Board business or education records if their content includes personally identifiable information about a student. Consequently, staff shall comply with a ~~District~~ Board request to produce copies of e-mail in their possession that are either public records or education records, or that constitute ESI that is subject to a litigation hold, even if such records reside on a computer owned by an individual staff member, or are accessed through an e-mail account not controlled by the ~~District~~ Board.

~~Retention~~

~~Pursuant to State and Federal law, e-mails that are public records or education records, and e-mails that are subject to a litigation hold shall be retained.~~

~~E-mail retention is the responsibility of the individual e-mail user. Users must comply with District guidelines for properly saving/archiving e-mails that are public records, student education records, and/or subject to a litigation hold. E-mails sent or received using the District's e-mail service may only be retained for thirty (30) days on the server. This retention is for disaster recovery and not to provide for future retrieval. The District does not maintain a central or distributed e-mail archive of e-mail sent and/or received. Any questions concerning e-mail retention should be directed to the Technology Director.~~

~~Unauthorized E-mail~~

~~The Board does not authorize the use of its Technology Resources, including its computer network ("network") to accept, transmit, or distribute unsolicited bulk e-mail sent through the Internet to network e-mail accounts. In addition, Internet e-mail sent, or caused to be sent, to or through the network that makes use of or contains invalid or forged headers, invalid or nonexistent domain names, or other means of deceptive addressing will be deemed to be counterfeit. Any attempt to send or cause such counterfeit e-mail to be sent to or through the network is unauthorized. Similarly, e-mail that is relayed from any third party's e-mail servers without the permission of that third party, or which employs similar techniques to hide or obscure the source of the e-mail, is also an unauthorized use of the network. The Board does not authorize the harvesting or collection of network e-mail addresses for the purposes of sending unsolicited e-mail. The Board reserves the right to take all legal and technical steps available to prevent unsolicited bulk e-mail or other unauthorized e-mail from entering, utilizing, or remaining within the network. Nothing in this policy is intended to grant any right to transmit or send e-mail to, or through, the network. The Board's failure to enforce this policy in every instance in which it might have application does not amount to a waiver of its rights.~~

~~Unauthorized use of the network in connection with the transmission of unsolicited bulk e-mail, including the transmission of counterfeit e-mail, may result in civil and criminal penalties against the sender and/or possible disciplinary action.~~

~~Authorized Use and Training~~

~~Pursuant to Policy 7540.04, staff and Board members using the District's e-mail system shall acknowledge their review of, and intent to comply with, the District's policy on acceptable use and safety by signing and submitting Form 7540.04 F1 annually.~~

~~Furthermore, staff and Board members using the District's e-mail system shall satisfactorily complete training, pursuant to Policy 7540.04, regarding the proper use and retention of e-mail annually.~~

~~Adopted 11/4/10~~
~~Revised 6/28/12~~
~~Revised 9/22/16~~

All staff shall annually receive training on this policy and acknowledge receipt and understanding of it by means of a written statement provided by the Superintendent.