ROANE COUNTY SCHOOLS

Policy ~~7540.03~~ 490 – ~~Student Technology~~ Acceptable Use of Technology by Students ~~and Safety~~

Revised policy and repeal of Policy 7540.06 (District-Issued Student E-mail Account), Policy 5136 (Personal Communication Devices), and Policy 5136.01 (Technology Resources and Other Electronic Equipment) 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 students and staff. The Board provides students with access to the Internet for limited educational purposes only and utilizes online educational services/apps to enhance the instruction delivered to its students.

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, and articulated expectations of student conduct as delineated in the Student Code of Conduct.~~ This policy ~~and its related administrative guidelines~~ and the Student Code of Conduct govern students' use of the ~~District's~~ County's technology and information resources and students' personal communication devices when they are connected to the ~~District~~ County's computer network, Internet connection, and/or online educational services/apps, or when used while the student is on Board-owned property or at a Board-sponsored activity ~~(see Policy 5136)~~.

~~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).~~

~~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.

~~At the discretion of the Board or the Superintendent, the technology protection measures may be configured to protect against access to other material considered inappropriate for students to access. The Board also utilizes software and/or hardware to monitor online activity of students 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 student who attempts to disable the technology protection measures will be subject to discipline.~~

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.

Parents are advised that a determined user may be able to gain access to services and/or resources on the Internet that the Board has not authorized for educational purposes. ~~In fact, it is impossible to guarantee students will not gain access through the Internet to information and communications that they and/or their parents may find inappropriate, offensive, objectionable, or controversial.~~ Parents of minors are responsible for setting and conveying the standards that their children should follow when using the Internet.

Pursuant to Federal law, students shall receive education about the following:

A. safety and security while using e-mail, chat rooms, social media, and other forms of direct electronic communications;
B. the dangers inherent with the online disclosure of personally identifiable information;
C. the consequences of unauthorized access (e.g., "hacking", "harvesting", "digital piracy", "data mining", etc.), cyberbullying and other unlawful or inappropriate activities by students online; and
D. unauthorized disclosure, use, and dissemination of personally identifiable information regarding minors.

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.~~

~~Students will be assigned a school e-mail account that they are required to utilize for all school-related electronic communications, including those to staff members, peers, and individuals and/or organizations outside the District, with whom they are communicating for school-related projects and assignments. Further, as directed and authorized by their teachers, they shall use their school-assigned e-mail account when signing-up/registering for access to various online educational services, including mobile applications/apps that will be utilized by the student for educational purposes.~~

Students are responsible for good behavior when using ~~District~~ County technology resources - i.e., behavior comparable to that expected of students when they are in classrooms, school hallways, and other school premises and school-sponsored events. Communications on the Internet are often public in nature. General school rules for behavior and communication apply. ~~The Board does not approve any use of its technology resources that is not authorized by or conducted strictly in compliance with this policy and its accompanying guidelines.~~

~~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.~~

Students may only use ~~District~~ County technology resources to access or use social media if it is done for educational purposes in accordance with their teacher's approved plan for such use.

~~Users~~ Students who disregard this policy ~~and its accompanying guidelines~~ may have their use privileges suspended or revoked, and disciplinary action taken against them.

~~Users~~ Students are personally responsible and liable, both civilly and criminally, for uses of ~~District~~ County technology resources that are not authorized by this policy ~~and its accompanying guidelines~~.

~~Based upon the acceptable use and safety guidelines outlined in West Virginia State Board of Education policy 2460, the State Superintendent, the 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.~~

~~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. 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.~~

~~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 students' use of District Technology Resources.~~

~~West Virginia State Board of Education policy 2460 – Education 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~~

~~Revised 9/16/08~~
~~Revised 5/10/12~~
~~Revised 6/28/12~~
~~Revised 11/19/15~~
~~Revised 9/22/16~~

District-Issued Student E-Mail Account
Students assigned a school email account are required to utilize it for all school-related electronic communications, including those to staff members and individuals and/or organizations outside the ~~District~~ County with whom they are communicating for school-related projects and assignments. Further, as directed and authorized by their teachers, they shall use their school-assigned email account when signing-up/registering for access to various online educational services, including mobile applications/apps that will be utilized by the student for educational purposes.

~~This policy and any corresponding guidelines serve to establish a framework for student's proper use of e-mail as an educational tool.~~

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. Students 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.

Students shall not send or forward mass e-mails, even if educationally-related ~~without prior approval of their classroom teacher or the Technology Director~~.

Students may join list servs or other e-mail services (e.g. RSS feeds) that pertain to academic work, provided the e-mails received from the list servs or other e-mail services do not become excessive. ~~If a student 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 classroom teacher, the 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~~ student become excessive.

Students are encouraged to keep their inbox and folders organized by regularly reviewing e-mail messages and purging e-mails once they are read and no longer needed for school.

~~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 non-existent 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 7540.03, students 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 7540.03 F1 annually.~~

~~Furthermore, students using the District's e-mail system shall satisfactorily complete training, pursuant to Policy 7540.03, regarding the proper use of e-mail annually.~~

Personal Communication Devices

"Personal communication devices" (PCDs) as used in this policy are defined ~~in Bylaw 0100~~ as those electronic devices which may, as whole or part of their function, allow for communication via wireless, wired, visual, or auditory means, to one or many other parties.

While students may possess PCDs in school, on school property, during after school activities (e.g., extra-curricular activities) and at school-related functions, they must be powered completely off (i.e., not just placed into vibrate or silent mode) and stored out of sight during school hours, during after school activities (e.g., extra-curricular activities), and on school buses or other Board-provided vehicles.

However, technology including, but not limited to, PCDs intended and actually used for instructional purposes (e.g., taking notes, recording classroom lectures, writing papers) ~~will~~ may be permitted, as approved by the classroom teacher ~~or the building principal~~. The use of a PCD under this paragraph to engage in non-educational-related communications is expressly prohibited.

Students may not use PCDs on school property or at a school-sponsored activity to access and/or view Internet web sites that are otherwise blocked to students at school.

During after school activities, PCDs shall be powered completely off (not just placed into vibrate or silent mode) and stored out of sight when directed by the administrator or sponsor.

Under certain circumstances, a student may keep his/her PCD "On" with prior approval from the building principal.

Except as authorized by a teacher, administrator or IEP team, students are prohibited from using PCDs during the school day, including while off-campus on a field trip, to capture, record and/or transmit the words or sounds (i.e., audio) and/or images (i.e., pictures/video) of any student, staff member or other person. Using a PCD to capture, record and/or

transmit audio and/or pictures/video of an individual without proper consent is considered an invasion of privacy and is not permitted. Students who violate this provision and/or use a PCD to violate the privacy rights of another person shall have their PCD confiscated and held until a parent/guardian picks it up, and may be directed to delete the audio and/or picture/video file while the parent/guardian is present. If the violation involves potentially illegal activity, the confiscated-PCD may be turned over to law enforcement.

The use of PCDs that contain built-in cameras (i.e., devices that take still or motion pictures, whether in a digital or other format) is prohibited in classrooms, gymnasiums, locker rooms, shower facilities, rest/bathrooms and/or swimming pool.

Students shall have no expectation of confidentiality with respect to their use of PCDs on school premises/property.

Students may not use a PCD in any way that might reasonably create in the mind of another person an impression of being threatened, humiliated, harassed, embarrassed or intimidated. ~~See Policy 5517.01 – Bullying and Other Forms of Aggressive Behavior.~~ In particular, students are prohibited from using PCDs to: (1) transmit material that is threatening, obscene, disruptive, or sexually explicit or that can be construed as harassment or disparagement of others based upon their race, color, national origin, sex (including sexual orientation/transgender identity), disability, age, religion, ancestry, or political beliefs; and (2) engage in "sexting" - i.e., sending, receiving, sharing, viewing, or possessing pictures, text messages, e-mails or other materials of a sexual nature in electronic or any other form. Violation of these prohibitions shall result in disciplinary action. Furthermore, such actions will be reported to local law enforcement and child services as required by law.

Students are also prohibited from using a PCD to capture, record, and/or transmit test information or any other information in a manner constituting fraud, theft, cheating, or academic dishonesty. Likewise, students are prohibited from using PCDs to receive such information.

Possession of a PCD by a student at school during school hours and/or during extra-curricular activities is a privilege that may be forfeited by any student who fails to abide by the terms of this policy, or otherwise abuses this privilege.

Violations of this policy may result in disciplinary action and/or confiscation of the PCD. The building principal will also refer the matter to law enforcement or child services if the violation involves an illegal activity (e.g., child pornography, sexting). Discipline will be imposed on an escalating scale ranging from a warning to an expulsion based on the number of previous violations and/or the nature of or circumstances surrounding a particular violation. If the PCD is confiscated, it will be released/returned to the student's parent/guardian after the student complies with any other disciplinary consequences that are imposed, unless the violation involves potentially illegal activity in which case the PCD may be turned over to law enforcement. A confiscated device will be marked in a removable manner with the student's name and held in a secure location in the building's central office until it is retrieved by the parent/guardian or turned over to law enforcement. School officials will not search or otherwise tamper with PCDs in ~~District~~ Board custody unless they reasonably suspect that the search is required to discover evidence of a violation of the law or other school rules. ~~Any search will be conducted in accordance with Policy 5771 – Search and Seizure.~~ If multiple offenses occur, a student may lose his/her privilege to bring a PCD to school for a designated length of time or on a permanent basis.

A person who discovers a student using a PCD in violation of this policy is required to report the violation to the building principal.

Students are personally and solely responsible for the care and security of their PCDs. The Board assumes no responsibility for theft, loss, or damage to, or misuse or unauthorized use of, PCDs brought onto its property.

Parents/Guardians are advised that the best way to get in touch with their child during the school day is by calling the school office.

Students may use school phones to contact parents/guardians during the school day when granted approval by an appropriate staff member.

~~*Technology Resources and Other Electronic Equipment*~~
~~While in some instances the possession and use of Technology Resources (as defined in Bylaw 0100) and other electronic equipment or devices by a student at school may be appropriate, the possession and use of such Technology Resources and other equipment or devices by students at school also may have the effect of distracting, disrupting and/or intimidating others in the school environment and leading to opportunities for academic dishonesty and other disruptions of the educational process.~~

~~Students may use the following Technology Resources and other electronic equipment/devices on school property only for educational or instructional purpose (e.g. taking notes, recording a class lecture, writing papers) with the teacher's permission and supervision:~~

~~A. laptops~~
~~B. tablets (e.g., iPad-like devices)~~
~~C. smartphones~~
~~D. e-readers (e.g., Kindle-like devices)~~
~~E. personal digital assistants (PDAs)~~

~~Students are prohibited from using Technology Resources and other electronic equipment or devices in a manner that may be physically harmful to another person (e.g. shining a laser in the eyes of another student). Further, at no time may any Technology Resources or other electronic equipment/device be utilized by a student in a way that might reasonably create in the mind of another person an impression of being threatened, humiliated, harassed, embarrassed, or intimidated. See Policy 5517.01 – Bullying. In particular, students are prohibited from using Technology Resources, a camera, or other electronic equipment/device to: (1) transmit material that is threatening, obscene, disruptive, or sexually explicit or that can be construed as harassment or disparagement of others based upon their race, national origin, sex (including transgender identity, sexual orientation, and gender identity), age, disability, religion, or political beliefs; and (2) send, share, view or possess pictures, text messages, e-mails or other materials of a sexual nature (i.e., sexting) in electronic or any other form. Violation of these prohibitions shall result in disciplinary action.~~

~~Furthermore, such actions will be reported to local law enforcement and child services as required by law.~~

~~Students are prohibited from using Technology Resources and other electronic equipment/devices to capture, record, or transmit test information or any other information in a manner constituting fraud, theft, or academic dishonesty. Similarly, students are prohibited from using Technology Resources and other electronic equipment and devices to capture, record, or transmit the words (i.e. audio) and/or images (i.e. pictures/video) of any student, staff member or other person in the school or while attending a school-related activity, without express prior notice and explicit consent for the capture and/or recording of such words or images. Using Technology Resources or other electronic equipment/devices to capture, record, or transmit audio and/or pictures/video of an individual without his/her consent is considered an invasion of privacy and is not permitted, unless authorized by the building principal. Technology Resources and other electronic equipment/devices are expressly banned from and may not be possessed, activated, or utilized at any time in any school situation where a reasonable expectation of personal privacy exists. These locations and circumstances include but are not limited to locker rooms, shower facilities, restrooms, classrooms, and any other areas where students or others may change clothes or be in any stage or degree of disrobing or changing clothes. The~~

~~building principal has authority to make determinations as to other specific locations and situations where possession of a camera or other electronic equipment/device is prohibited.~~

~~Public Events Exception: Photography and video recordings shall be permitted at scheduled public events where the same have been traditionally allowed. This public events exception shall apply, for example, to sporting events. A notice shall be posted at all events which qualify for this exception.~~

~~Official School Photography and Videography: Photography and video recordings shall be permitted where student are acting in an official school-related capacity. This exception would include, for example, school yearbook photographs, school newspapers, sports team game filming, etc. The faculty sponsor for each official school-related activity that qualifies for this exception will be notified in writing by the building principal.~~

~~Unauthorized Technology Resources and other electronic equipment and devices will be confiscated from the student by school personnel and disciplinary action taken.~~

~~If Technology Resources or other electronic equipment/device is confiscated, it will be released/returned to the student's parent/guardian only.~~

~~Any Technology Resources or other electronic equipment/device confiscated by District staff will be marked in a removable manner with the student's name and held in a secure location in the building's central office until it is retrieved by the parent/guardian. Technology Resources or other electronic equipment/devices in District custody will not be searched or otherwise tampered with unless school officials reasonably suspect that the search is required to discover evidence of a violation of the law or other school rules (e.g. a student is observed using a camera in a prohibited area). Any search will be conducted in accordance with Policy 5771 – Search and Seizure.~~

~~Students are personally and solely responsible for the care and security of any Technology Resources and other electronic equipment or devices they bring to school. The Board assumes no responsibility for theft, loss, damage, or vandalism to electronic equipment and devices brought onto its property, or the unauthorized use of such devices.~~

<u>All students shall annually receive instruction on this policy and acknowledge receipt and understanding of it by means of a written statement provided by the Superintendent.</u>