WV Code §§18-5-19, 18-5A-2(j)(5)
Evans v. Hutchinson, 158 WV 359, 364 (1975)

8.8 ACCEPTABLE USE OF COMPUTER TECHNOLOGY AND NETWORKS

The Board is committed to the effective use of technology to both enhance the quality of student learning and the efficiency of Board operations. However, use of the Board's network and technology resources is a privilege, not a right.

The Putnam County Schools Technology Team shall develop written technology procedures which provide guidance to staff and students concerning the safe, appropriate, and ethical use of the Board's network(s) based on WVBOE policy regarding the use of electronic resources, technologies, and the Internet.

The technology procedures shall also inform both staff and students about disciplinary actions that will be taken if Board technology and/or network(s) are abused in any way or used in an inappropriate, illegal, or unethical manner. Unacceptable use of technology includes, but is not limited to:

A. transmission or use of any material in violation of any federal or state law or regulation;
B. use for commercial activities, product advertising, or political lobbying;
C. transmission or use of any obscene, pornographic, or sexually explicit material;
D. transmission or use of any type of virus or malicious file or computer code to disable or disrupt service;
E. illegally accessing or attempting to access any school, district, or state e-mail, electronic ID/password, data, system files, online resources, or equipment of the school that does not belong to the user;
F. hacking, cracking, vandalizing, and other unlawful online activities;
G. disclosing, using, or disseminating personal information regarding students;
H. cyberbullying, hate mail, defamation, harassment, discriminatory jokes and remarks, and other unauthorized behaviors as defined in other Board policies; and/or
I. "sexting," the electronic transmission of sexual messages or pictures.

Further, safeguards, methods, and instructional models established by WVBOE policy to address Internet safety will be implemented and documented by the Board. All network access to the Board-provided Internet shall be filtered through WVDE and/or county system filters to decrease the risk of students accessing inappropriate or harmful material. Accordingly, students shall be educated about appropriate online behavior including, but not limited to, 1) interacting with other individuals through electronic mail, on social networking websites, and in chat rooms and 2) recognizing what constitutes cyberbullying, understanding cyberbullying is a violation of Board policy, and learning appropriate responses if they are victims of cyberbullying.

Student use of Internet-related or web-based applications must be authorized by an educator and the parent/guardian through a signed Acceptable Use Authorization form. Appropriate adult supervision of Internet use must be provided. While WVDE does filter Internet traffic, filtering software is not 100% effective. Deliberate and consistent monitoring of student use of the Internet and technologies is vital to prevent access to inappropriate and harmful materials. While classroom educators have primary contact

with students, acceptable and appropriate use of online resources, technologies, and the Internet is the responsibility of all county staff and employees.

The acceptable and appropriate use of telecommunications and/or access to the Internet and digital resources is an extension of the educator's responsibility in his/her classroom. Educators occupy a position of trust and stand in the place of a parent/guardian while a student is in school. Therefore, it is the educator's responsibility to ensure classroom activities focus on appropriate and specific learning goals and objectives when using Internet-related technologies. It is the educator's responsibility to avoid using technology in such a manner that places him/her in a position to abuse that trust.

Collaboration, resource sharing, and dialogue between the educational stakeholders (teachers, students, and/or parents) may be facilitated by the use of social media and other electronic communication. Such interactivity outside of the school walls can enhance classroom instruction. However, a clear line must be drawn between personal and professional/educational social networking to protect the safety of the students and the integrity of educational professionals and service staff. Use of social media and electronic communication must support the educational process and follow county technology procedures. Educators are discouraged from using personal accounts to contact students.

Professional development regarding the responsible use of the Internet and other technologies will be provided to employees and students. Employees and students who complete the training and sign Acceptable Use Authorization forms may be provided with appropriate usernames and passwords to access the Board's network(s) and technologies.

Employees and students who receive training on WVBOE Policy 2460 may apply for a state e-mail account and password. A state e-mail address may be required to participate in state online courses, to receive information distributed through state and county distribution lists and listservs, and to access county servers and websites. Use of personal e-mail accounts to contact staff, students, and parents is discouraged. Students must use a state or county educational e-mail account for school work and communication.

All information stored within the state's and Board's computers, servers, and other technology devices is the property of the state, Board, or school. Users of the Board's equipment and networks have no expectations of privacy with respect to its content.

The West Virginia Education Information System (WVEIS) is to be used exclusively for the business of the Board and its schools. All staff must maintain the confidentiality of student data in accordance with The Family Educational Rights and Privacy Act (FERPA).

The Board recognizes the educational benefits of school personnel and students publishing information on the Internet. The Board also recognizes the importance of guidelines that address content, overall responsibility, quality, copyright laws, and student protection. Standards for web publishing are found in section 8.9 - Web Publishing. Written permission from the student's parent/ guardian must be obtained prior to publishing any student information or work to the Internet.

The Board shall follow the guidelines of federal and state law, the Children's Internet Protection Act (CIPA), and the Children's Online Privacy Protection Act federal statues (COPPA). Unauthorized or unacceptable use of the Internet or educational technologies as part of an educational program by students, educators, or staff may result in suspension or revocation of such use and/or disciplinary actions involving local, county, state, or federal agencies.

Students and staff are prohibited from using county or personally owned devices to capture, record or transmit the sounds (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, recording, or transmission of such words or images. Taking or transmitting audio and/or pictures/video of an individual, without his/her consent, may be an invasion of privacy and is not permitted, unless authorized by the building principal.

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.

Official School Photography and Videography Exception

Photography and video records shall be permitted where students 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.

Technology may not be used in any way that might reasonably be interpreted by others as an attempt to threaten, humiliate, bully, harass, embarrass, or intimidate another person. The use of any camera device (i.e. devices that take still or motion pictures, whether in a digital or other format) is prohibited in locker rooms and bathrooms.

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

The Putnam County Schools Technology Team shall annually review all technology procedures and forms and report any recommended and/or mandatory changes, amendments, or revisions to the Superintendent and Board.

Children's Internet Protection Act
Children's Online Privacy Protection Act
The Family Educational Rights and Privacy Act
WVBOE Policy 2460

8.9 WEB PUBLISHING

The Board recognizes the educational benefits of school personnel and students publishing information on the Internet. The Board also recognizes the importance of guidelines that address content,

overall responsibility, quality, technical standards, and student responsibilities. This policy complies with standards more fully addressed in WVBOE policy.

Webpages/sites must reflect the professional image of the Board, its employees, and students. The content of all pages must be consistent with the Board's Mission Statement, and staff-created webpages/sites are subject to prior review and approval of the Superintendent. Student-created webpages/sites are subject to section 8.8 - Use of Computer Technology and Networks. The creation of webpages/sites by students must be done under the supervision of a professional staff member.

The purpose of webpages/sites hosted by the Board is to educate, inform, and communicate with the educational community. The Board provides website hosting for all school websites/pages. While schools may publish pages to other web hosting sites, all pages should have a link on and to the Board's website. The Board retains all proprietary rights related to the design of websites that are hosted on the Board's servers, absent written agreement to the contrary.

Development of webpages/sites is a worthwhile learning experience for students. Parents and community members may be excellent resources for this experience. While students, parents/guardians, and community members may participate in the development of the school website/page, a school employee must be ultimately responsible for posting information to the webpage/site and for webpage/site security.

Written parental/guardian permission must be obtained before student names, images, or work may be published on the Internet. No personal information, including home address and/or telephone, will be published. Students who want their class work to be displayed on any Board website must have written parental permission and expressly license its display without cost to the Board.

Under no circumstances is a staff created webpage/site, including a personal webpage/site, to be used to post student progress reports or grades. The Board maintains its own websites (e.g., Engrade and Echo) that employees are required to use for the purpose of conveying grade and progress information to students and/or parents/guardians.

A staff member is prohibited from requiring students to go to the staff member's personal webpage/site (including, but not limited to, their Facebook page) to check grades, obtain class assignments and/or class-related materials, and/or turn in assignments.

Business/commercial links should be limited to business partners or websites that contain educational or technical support. Advertising of commercial products is forbidden. Under no circumstances is a Board webpage/site to be used for commercial purposes, advertising, or political lobbying or to provide financial gains for any individual. All links and content included on Board webpages/sites must meet the above criteria and must comply with copyright, intellectual property, and state, federal, and international law.

WV Code §§St. R. 126-41-1, 126-94-1
WVBOE Policies 2460, 4350

8.10 NETWORK ACCESS FROM PERSONALLY OWNED COMPUTERS AND/OR OTHER WEB-ENABLED DEVICES

In order to provide increased access to educational opportunities and to support the educational process, the Board permits personally owned devices to access its Internet in accordance with their standards. Personally owned devices (PODs) include, but are not limited to, portable computers, web-enabled mobile devices, and cell phones with data plans.

Board members, county system employees, and students, as well as contractors, vendors, and agents of the county, may use their personally owned devices to access the Board-provided Internet while they are on-site at any county facility, provided that 1) the use supports the educational process, 2) the user registers the POD with the building administrator, and 3) the use complies with E-rate and Board policies and procedures. Elementary and middle school students must complete a training course with a parent/guardian before permission will be granted to bring a POD.

Connecting to the Board-provided Internet shall be in accordance with standards established by the Board. Students must use Board-provided Internet for instructional activities; the personal data plan on the POD should be turned off during classroom instruction.

Using a personally owned device to establish a wireless network, including tethering or mobile hotspots, is prohibited. A POD may not be used at any time on school property or at a school-sponsored activity for the purpose of accessing and/or viewing Internet websites that are otherwise blocked at school. Access to county servers is not permitted via personally owned devices.

By bringing a POD onto the property of the Board or to a school-sponsored event or activity, the owner assumes sole responsibility for safety and care of such POD. The Board assumes no responsibility for theft, loss, damage, or vandalism to any personally owned device brought onto its property or the unauthorized use of such device. The Board is not liable for any charges incurred by the user of the POD.

Personally owned devices using the Board-provided Internet should have current operating system updates, appropriate anti-virus software, and other security features enabled. County personnel will provide security assistance connecting to the Board-provide Internet. County personnel will not load software onto or repair or maintain any POD.

Students may use approved PODs in the classroom as a tool to support the learning process according to rules defined by the teacher, school, and/or Board.

When permitted by school rules and as long as they do not create a distraction, disruption, or otherwise interfere with the educational environment, students may use PODs before and after school, during their lunch break, during after-school activities (e.g., extracurricular activities), and at school-related functions. Students may use PODs while riding to and from school on a school bus or other vehicle provided by the Board or on a school bus or Board-provided vehicle during school sponsored activities, at the discretion of the bus driver, classroom teacher, or sponsor/advisor/coach. Distracting behavior that creates an unsafe environment will not be tolerated.

When directed to do so by a school employee, personally owned devices shall be powered completely off (not just placed into vibrate or silent mode) and stored out of sight. The requirement that a POD must be powered completely off will not apply in a circumstance when a student obtains prior, written approval from the building administrator (e.g., an ill family member or a personal health condition).

Student possession of a POD on school property or during a school-sponsored event is a privilege that may be forfeited by any student who fails to abide by the terms of this policy or otherwise engages in misuse of this privilege.

Violations of this policy may result in disciplinary action and/or confiscation of the device. The building administrator may also refer the matter to law enforcement if the violation involves an illegal activity (e.g., child pornography or cyberbullying). 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 device is confiscated, it will be released/returned only to the student's parent/guardian. Any device confiscated by school staff will be marked with the student's name and held in a secure location in the building's office until it is retrieved by the parent/guardian. Personally owned devices in county custody will not be searched or otherwise tampered with unless reasonable suspicion exists that warrants the same. If a student violates the terms of this policy, he/she may lose his/her privilege to bring a POD to school for a designated length of time or on a permanent basis, as the circumstances warrant.