R 3-32-4-3

PRESTON COUNTY SCHOOLS—NETWORK AND INTERNET ACCEPTABLE USE POLICY (AUP)

To meet the goal that every high school graduate will be prepared fully for college, other post-secondary education or gainful employment the Board believes that a technology infrastructure should be present in the County schools. In order to meet this goal, 21st century technologies and software resources shall be provided in grades prekindergarten through 12.

The Preston County Board of Education believes that technology must be interwoven with educational improvements and personalized learning to accomplish educational goals, increase student achievement and educator efficacy, and provide increased opportunities for lifelong learning.

This policy applies equally to students and school personnel. To the extent practicable, technology resources shall be used:

- To maximize student access to learning tools and resources at all times including during regular school hours, before and after school or class, in the evenings, on weekends and holidays and for public education, non-instructional days and during vacations; and
- For student use for homework, remedial work, independent learning, career planning and adult basic education.

Educational Purposes

The Preston County Board of Education agrees with the general goals articulated in *SBP 2460 Educational Purposes and Acceptable Use of Electronic Resources, Technologies and the Internet* and adopts the following educational purposes as guidelines to be followed in the Preston County Schools:

- An effective public education system develops students who are globally aware, engaged with their communities, and capable of managing their lives and careers to succeed in a digital world.
- Students of all ages and educators as lifelong learners require the necessary skills and access to technology tools to take responsibility for their own learning, to be actively involved in critical thinking and problem solving, to collaborate, cooperate, and to be productive citizens. West Virginia students must become proficient in college- and career-readiness standards to succeed and prosper in life, in school, and on the job.
- Technology must be interwoven with educational improvements and personalized learning to accomplish educational goals, increase student achievement and educator efficacy, and provide increased opportunities for lifelong learning.
- To promote student learning, teachers must be equipped to fully integrate technology to transform instructional practice and to support student acquisition of technology skills necessary to succeed, to continue learning throughout their lifetimes, and to attain self-sufficiency.
- The state, districts, and schools will use electronic resources as a powerful and compelling means for students to learn core and elective subjects and applied skills in relevant and rigorous ways to advance learning as referenced in W. Va. Code §18-2e-7, W. Va. 126CSR44N, WVBE Policy 2520.14, West Virginia College- and Career-Readiness Standards for Technology and Computer Science (Policy 2520.14), W. Va. 126CSR42, WVBE Policy 2510, Assuring the Quality of Education: Regulations for Education Programs, and W. Va. 126CSR44A et ~~al~~ seq., WVBE Policy 2520 series.
- Learning powered by technology should enable students to achieve at higher academic levels, master digital content and technologies, access and manage information, communicate effectively, think critically, solve problems, work productively as individuals and collaboratively as part of a team, acquire new knowledge, access online assessment systems, and demonstrate personal accountability, productivity, and other self-directional skills.
- The use of instructional technology should provide greater student access to advanced and additional curricular offerings~~,~~ including quality virtual courses and online educational tools and resources.
- Teachers should integrate high quality digital content and assessment resources with curriculum to personalize learning.
- Technology will enable educators to participate in online professional development, access digital resources and platforms, utilize educational data, and deliver instruction through blended learning and other virtual options. The acceptable use of digital resources and devices is necessary to support a personalized learning landscape and other district and state educational policies.
- The promotion of acceptable use in instruction and educational activities is intended to both provide a safe digital environment, and meet **Federal Communications Commission** (FCC) guidelines and E-rate audits.

R 3-32-1 Digital Citizenship

It is incumbent upon the students and staff to work cooperatively to assure that all technology and digital resources will be utilized appropriately, safely and civilly. Digital citizenship represents more than technology literacy. Successful, technologically fluent digital citizens live safely and civilly in an increasingly digital world and use technology responsibly. They recognize that information posted on the Internet is public and permanent and can have a long-term impact on an individual's life and career.

Digital/Network Code of Conduct

Users are expected to abide by the generally accepted rules of digital/network etiquette. These include, but are not limited to, the following:

- Be polite. Do not write or send abusive messages to others.
- Use proper English and appropriate language; avoid "Netspeak." Do not swear; do not use vulgarities or other inappropriate language.
- Use extreme caution when revealing personal information, including a home address and phone number, on web sites, videos, social media, other digital communication platforms, e-mail, or as content on any other electronic medium.
- Do not reveal, on any electronic medium, personal information about another individual.
- Do not use the Internet in a way that would disrupt the use of the Internet by others.
- Electronic educational material containing confidential student information shall be stored only in secure locations consistent with federal, state, and local privacy regulations. Electronic educational material containing no confidential student information, including but not limited to, lesson plans, worksheets, primary source documents, and other materials used for instruction, may be stored in appropriate locations but should follow state/district guidelines.
- Educators electing to use third party classroom based applications should carefully review the terms of service and privacy policies prior to use for those applications to ensure consistency with best practice. For use of applications with students younger than 13 years of age, recommended best practice is to obtain parental consent prior to use and/or entering any student data. All use of third party applications must

  be consistent with local policy/guidelines, Family Educational Rights and Privacy Act (20 U.S.C. §1232g; 34 CFR Part 99) FERPA), W. Va. Code §18-2-5h, and W. Va. 126SR94, WVBE
- Keep educational files and e-mail messages stored on servers to a minimum.
- Activate the appropriate automatic reply message and unsubscribe to listservs if account is to be unused for an extended period of time.

- Appropriate permission shall be obtained prior to publishing student pictures or names on class, school, or district web sites or other publications, provided that such information is not designated as directory information under district policy. All releases of information designated as directory information under district policy must comply with parental opt-out provisions as described in the FERPA and WVBE Policy 4350. (Also see *File: 11-19. Collection, Maintenance and Disclosure of Student Data)*
- Notify the appropriate school authority of any dangerous or inappropriate information or messages encountered.

Digital Security

Students and staff members who identify a security problem on the system must notify a system administrator immediately.

- Users must not demonstrate the problem to users other than school, district and/or state officials responsible for implementing the privacy incident response protocol
- Users must not use another individual's account or give their passwords to others. Unauthorized attempts to log into the system as a system administrator may result in revocation of user privileges based on state, district or school policies.
- Any user identified as a security risk or having a history of problems with other computer systems may be denied access by the appropriate disciplinary authority.

R 3-32-2 Accountability and Responsibility

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 or guardian while a student is in school (WVC § 18A-5-1(a). Therefore, it is the educator's responsibility to ensure classroom activities focus on appropriate and specific learning goals and objectives for personalized learning when using Internet-related technologies.

Student use of Internet-related or web-based applications must be authorized by the educator and parent or guardian through File: R 3-32-4 -2 Internet and Telecommunications Access Consent and Waiver Form. It is also the educator's responsibility not to use electronic technologies in a manner that risks placing him/her in a position to abuse that trust. Even though "educators" are the ones who come in daily classroom contact with students, acceptable and appropriate uses of online resources, technologies and the Internet is a responsibility of all educational staff and employees.

Adult use of Internet-related or web-based applications must be authorized through the *R 3-32-4-2 Internet and Telecommunications Access Consent and Waiver Form*. Access Passwords cannot be issued to adult users until this form is completed and returned.

R 3-32-3 Use of Electronic Resources, Technology and the Internet

While working within the framework and within the jurisdiction of the State Board of Education and its agents (local school districts), the use of various electronic resources, technology and the internet is a privilege and not a right. Therefore, the following guidelines and restrictions must be read carefully by all users.

- Unauthorized or unacceptable use of the Internet or any safety violations as part of an educational program by students, educators or staff may result in suspension or revocation of access privileges...
- Each student who will access the Internet will be provided acceptable use training and shall have an acceptable use form, signed by a parent or legal guardian, on file at the district/school.
- School personnel shall also receive acceptable use training.
- The WVDE provides the network system, e-mail accounts and Internet access as tools for education and administration in support of the WVBE's mission. Therefore, users should have no expectation of privacy; and the WVDE reserves the right to monitor, inspect, investigate, copy, review and store, without prior notice, information about the content and usage of any and all information transmitted or received in connection with networks, e-mail use, and web-based tools.
- No student or staff user should have any expectation of privacy when using the district's network or equipment. The WVDE reserves the right to disclose any electronic message, files, media, and other information, to law enforcement officials or third parties as appropriate.
- No temporary accounts will be issued, nor will a student use an Internet account not specifically created for him or her. Based upon the acceptable use and safety guidelines outlined in this document, WVDE, State Superintendent of Schools and WVDE system administrators will determine what appropriate use is, and their decision is final.
- Violation of use policies could result in loss of access, personal payment of fees incurred, employment discipline, licensure revocation and/or prosecution. Other consequences for students may ~~also~~ be found in Policy 4373.
- The system administrator and/or local teachers may deny users access for inappropriate use. Additionally, violation of use policies could result in loss of access, personal payment of fees incurred, employment discipline, licensure revocation and/or prosecution. Other violations may also be found in *SBP 4373.*
- Administrative information systems, including WVEIS, are to be used exclusively for educational purposes. Ownership of student, personnel, and financial records remains with the agency with primary responsibility for maintenance of the information. WVDE reserves the rights to access data maintained in or transmitted over state supported information systems and disclose it as appropriate for legitimate purposes. All staff must maintain the confidentiality of student data in accordance with FERPA and Policy 4350.
- Employees may not attempt to gain access to another employee's files in the WVDE's information systems. However, the WVDE reserves the right to enter an employee's information system files whenever there is a business need to do so.
- These guidelines may be superseded by FERPA and other appropriate federal and state laws to the extent that such laws are more restrictive.

R 32-3-4 Internet and Telecommunication Acceptable Use Procedures

The Preston County School System embraces the use of technology to promote educational excellence, resource sharing, assist innovative instruction; provide electronic access to a wide range of information and the ability to communicate. The use of the electronic resources, technologies and the Internet must be in support of education and consistent with the educational goals, objectives and priorities of the WVBE. Use of other networks or computing resources must comply with the rules appropriate for that network and for copyright compliance. Users must also comply with the rules and regulations of the network provider(s) serving West Virginia counties and schools.

As the use of telecommunication networks by students increase, there is a need to clarify acceptable use and safety of those networks and to include federal regulations from the Children's Online Privacy Protection Act (COPPA) and the Children's Internet Protection Act (CIPA). The use of telecommunications and/or access to the Internet is an extension of the students' responsibility in the classroom and must follow all federal and state laws as well as state and local policies.

State, district and school-owned technologies are to be used to enhance learning and teaching as well as improve the operation of the district and school. Safety measures must be enforced to carry out policies at the state, RESA, county, and school to implement the intent of CIPA, COPPA, E-rate guidelines, FERPA, and any other applicable state and federal statute and policy. (See also *SBP 4373* and WVC §18-2C-2.)

The use of the Internet as part of an educational program is a privilege, not a right, and inappropriate or unauthorized use or safety violations could result in revocation or suspension of that privilege. Each student who will access the Internet will be provided acceptable use training and shall have an acceptable use form, signed by a parent or legal guardian, on file.

Acceptable network use by students and staff includes the following:

- Creation of files, projects, and various media products using network resources in support of student personalized academic learning and educational administration;
- Appropriate participation in school-sponsored sites and online groups;
- The online publication of educational material for instructional purposes and, with parental permission, student work. As required by copyright law, external sources must be cited.
- Incidental personal use in accordance with all district/school policies and guidelines.

R 32-3-5 Unacceptable use of the Internet and Telecommunications

While the Board always prefers to address its policies in positive terms, it is essential that students and staff be made aware that inappropriate use or transmission of any material in violation of any U.S. or state law, State Board Policy, county policy or regulation is prohibited. This includes, but is not limited to, copyrighted material, threatening, abusive, or obscene material, or material protected by trade secrets. Such inappropriate behavior shall be met with zero tolerance.

In addition, use for commercial activities by for-profit institutions is not acceptable. Use for product advertisement or political lobbying is also prohibited. Illegal activities and privacy and safety violations of COPPA, CIPA and FERPA are strictly prohibited. Specific examples of unacceptable and/or unauthorized use include, but are not limited to:

Specific examples of unacceptable and/or unauthorized use include, but are not limited to:

- Inappropriate use or transmission of any material in violation of any federal 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 not acceptable.
- Use for product advertisement or political lobbying is also prohibited.
- Illegal activities and privacy and safety violations of COPPA, CIPA, and FERPA are strictly prohibited.
- Viewing, creating, accessing, uploading, downloading, storing, sending, or distributing obscene, pornographic or sexually explicit material.
- Downloading, uploading and/or executing viruses, worms, Trojan horses, time bombs, bots, malware, spyware, SPAM, and changes to tools used to filter content or monitor hardware and software.
- Illegally accessing or attempting to access another person's data or personal system files or unauthorized access to other state/district/school computers, networks and information systems.
- Using e-mail and other electronic user identifications (IDs)/passwords other than one's own or for unauthorized purposes. Students and staff are responsible for all activity on their account and must not share their account IDs and passwords.
- Supplying your password to others.
- Storing passwords in a file without encryption.
- Using the "remember password" feature of Internet browsers and e-mail clients.
- Leaving the computer without locking the screen or logging off.
- Corrupting, destroying, deleting, or manipulating system data with malicious intent.
- Requesting that inappropriate material be transferred.
- Violating safety measures when using any form of electronic communications.
- Hacking, cracking, vandalizing or any other unlawful online activities.
- Disclosing, using, or disseminating personal information regarding students.
- Cyberbullying, hate mail, defamation, harassment of any kind, discriminatory jokes and remarks and other unauthorized uses as referenced in, including but not limited to, Policy 4373 and other applicable federal and state statutes.
- Personal gain, commercial solicitation and compensation of any kind.
- Any activity which results in liability or cost incurred by the district.
- Unauthorized downloading, copying, installing and/or executing gaming, audio files, video files or other applications (including shareware or freeware).
- Campaigning, lobbying, or other activity via state supported platforms in support or opposition for political activity or issues, including but not limited to, ballot measures, candidates, or legislative proposals.
- Information posting, sending or storing information that could endanger others.
- Engaging in plagiarism or reproducing or repurposing media without permission.
- Attaching unauthorized equipment to the district or school networks or network connect devices. Any such equipment may be confiscated and turned over to law enforcement officers for a potential violation of WVC §61-3C-5, Unauthorized Access to Computer Services.
- Attaching unauthorized equipment or making unauthorized changes to the state backbone network. Unauthorized equipment may be confiscated and may turned over to law enforcement officers for a potential violation of W. Va. Code § 61-3C-5, Unauthorized Access to Computer Services. Only WVDE network personnel may authorize changes which affect the state backbone network.
- Vandalizing technology equipment or data including but is not limited to, uploading, downloading, or creating computer viruses or malware. Vandalism may result in revocation of user privileges and/or prosecution.
- Uses related to or in support of illegal activities will be reported to authorities.
- It is unacceptable to give administrative responsibilities for a server with a wide area network or Internet connection to a current PreK-12 student outside of a laboratory environment, as with career and technical education computer related courses.

R 3-32-4-1 Internet and Telecommunications Student Access Consent and Waiver Form

---

Agreement and Parent Permission Form

After reading the attached summary of Preston County Schools policies, please complete this form to indicate that you agree with the terms and conditions of those policies. The signatures of both student and parent/guardian are mandatory before Internet access may be granted. Use of the telecommunications network or telecommunication must be in support of education and/or research or for school business, support of the West Virginia Content Standards and Objectives and be in accordance with all Preston County Board of Education policies and *SBP 2460 Educational Purposes and Acceptable use of Electronic Resources, Technologies and the Internet.*

School Name_____

STUDENT SECTION

I have read the attached summary of Preston County Schools policies concerning all computer usage. I agree to follow the rules contained in these policies. I understand that if I violate the rules my privileges may be terminated or other disciplinary action taken.

Student Name (please print)_____ Grade: _____

Student's Signature: _____ Date: _____

PARENT SECTION

I have read the attached summary of Preston County Schools policies the policies for use of telecommunications in my child's school and have discussed this with my son/daughter. I understand that this access is for educational purposes only, and that it is the responsibility of my child to restrict his/her use to the classroom projects/activities assigned by the teacher. I also understand that my child cannot hold the teacher responsible for intentional infractions of the above rules.

Parent/Guardian (please print) _____

Parent/Guardian (signature) _____ Date_____

SCHOOL INTERNET WEBSITE STUDENT INFORMATION

I hereby **give my permission** to use the following information on the school website and/or in local media publications. Initial all that you approve.

_____ Student's first name _____ Student's photo

_____ Student in group photo _____ Student's work

PLEASE INITIAL IF YOU DO **NOT** AUTHORIZE ANY PHOTOS OR NAME INFORMATION ON THE SCHOOL

WEBSITE AND/OR IN LOCAL MEDIA PUBLICATIONS: _____

This form will be kept in the school listed above. It will not be transferred to another school. Please read the attached summary of Preston County Schools policies. The span of this agreement will be from the signature date until September 1, 2019.

PRESTON COUNTY SCHOOLS

731 Preston Drive
Kingwood, WV 26537

Steve Wotring, Superintendent
Brad Martin, Asst. Superintendent **(304) 329-0580**
Ange Varner, Asst. Superintendent **(304) 329-0720 ext. 225**

8/21/18

- TO BE COMPLETED FOR NEW STUDENTS/STAFF OR THOSE WITH UPDATED CONTACT INFORMATION (**NOT REQUIRED TO COMPLETE IF YOU ARE CURRENTLY RECEIVING CALLS AT APPROVED AND DESIRED TELEPHONE NUMBERS AND/OR EMAIL ACCOUNTS**).

Dear Parent / Guardian or Staff Member:

Due to the passage of the Telephone Consumer Protection Act by the Federal Communications Commission (FCC), automated calling systems such as the School Messenger cannot be used for non-emergency purposes without express written consent of individuals. In order to comply with this legislation, Preston County Schools has or will discontinue all non-emergency automated calls (including absence verification calls) until written consent of parents and staff can be collected and documented. Please review the permission slip below and indicate your approval to receive nonemergency messages via the School Messenger automated calling system from Preston County Schools. Upon receipt of this document, your account will be updated accordingly within the system as per your request. If you have questions about this notification, please contact the Preston County Board of Education at (304) 329-0580 ext. 225. Permission updates can also be completed online at the following link: http://www.prestonboe.com/forms/schoolmess.html

Student / Staff Name:_____

Parent/Guardian Name:_____

School Attending / Work Site:_____

Preferred Contact Number:_____

Preferred Contact Email (Optional):_____

I give my permission to receive non-emergency messages from Preston County School district at the following phone number(s) listed above via call, text or email by way of an automated dialing software, such as School Messenger.

_____ _____

(signature) **(date)**