R 3-32-4-1 Internet and Telecommunications 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.

User Name (please print)_____ Grade: _____

User'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 WEB SITE STUDENT INFORMATION:

I hereby give my permission to use the following information on the school web site. Initial all that you approve.

_____ Student's first name _____ Student's last name _____ Student's photo

_____ Student in group photo _____ Student's work

MEDIA & PUBLICITY APPROVAL RELEASE

I hereby grant permission for my child's name, voice, and/or picture to appear in local newspapers, on local television, or on local radio stations.

_____ (parent signature) _____ (date)

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.

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.

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 develop proficiency in 21st century content, technology tools, and learning skills to succeed and prosper in life, in school, and on the job.

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. 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:

- To promote student learning, educators 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.
- 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 increasing student access to quality virtual courses and online distance educational tools, than could be provided efficiently through traditional on-site delivery formats.
- Educators should integrate technology resources to personalize learning, enhance instruction, implement multiple technology-based learning strategies, implement high quality digital content and assessments, and utilize digital resources, technologies, and the Internet in the classroom.
- 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 provide a safe digital environment, as well as 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 Etiquette

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, blogs, podcasts, videos, wikis, 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 (e.g., downloading huge files during prime time; sending mass e-mail messages; annoying other users).
- 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.
- Only publish student pictures or names on class, school or district web sites that are part of the district/school directory information or when appropriate permission has been obtained. (Also see *File: 11-19 Collection, Maintenance and Distribution 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 other users.
- 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 will result in revocation of user privileges based on state, county 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.
- The WVDE is the proprietor of a class B license of Internet Protocol (IP) addresses. These addresses include 168.216.000.001 through 168.216.255.255. All addresses are assigned, maintained and managed by the WVDE. Any unauthorized use is strictly prohibited

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 *R 3-32-4-1 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/appropriate uses of online resources, technologies and the Internet is a responsibility of **all** educational staff and employees.

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 such use.
- 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 county/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, including student mastery of rigorous subject matter content and acquisition of global skills. 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:
  - The network and system files;
  - User files and disk space utilization;
  - User applications and bandwidth utilization;
  - User document files, folders and 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.

- No student or staff user should have any expectation of privacy when using the district's network. The WVDE reserves the right to disclose any electronic message, files, media, etc., 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 that allows anonymous posting. Based upon the acceptable use and safety guidelines outlined in this document, WVDE, State Superintendent of Schools and provider(s) system administrators will determine what appropriate use is, and their decision is final.
- 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.*
- The WVDE's administrative information systems, including the West Virginia Education Information System (WVEIS), are to be used exclusively for the business of the respective state, district (county) and school organizations. All information system data are records of the respective organizations. The
  WVDE reserves 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) (20 U.S.C. § 1232g; 34 CFR Part 99).
- For reasons of privacy, 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.
- Any of these guidelines are to be cognizant of and superseded by FERP A and other appropriate federal and state laws.
- The WVDE reserves the right to disclose any electronic message, files, media, etc., to law enforcement officials or third parties as appropriate.
- The WVDE reserves the right to enter an employee's information system files whenever there is a business need to do so.

R 3-32-4 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 be in compliance 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 technology is 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, videos, web pages and podcasts using network resources in support of student personalized academic learning and educational administration;
- Appropriate participation in school-sponsored blogs, wikis, web 2.0+ tools, social networking sites and online groups;
- With parental permission, the online publication of original educational material, curriculum related materials and student work. Sources outside the classroom or school must be cited appropriately;
- Staff use of the network for incidental personal use in accordance with all district/school policies and guidelines.

At no time should a student be given administrative responsibilities for a server with a wide area network or Internet connection.

R 3-32-5 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:

- 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, SP AM, etc., and changes to tools used to filter content or monitor hardware and software.
- Using e-mail and other electronic user IDs/passwords other than one's own. Passwords are the first level of security for a user account. E-mail and system logins and accounts are to be used only by the authorized owner of the account, for authorized purposes. Students and staff are responsible for all activity on their account and must not share their account IDs and passwords.
- 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.
- Supplying your password and user information to any electronic request or sharing them with others via any other communications.
- 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 and/or security measures when using e-mail, chat rooms, blogs, wikis, social networking sites, Web 2.0 tools and other forms of electronic communications.
- Hacking, cracking, vandalizing or any other unlawful online activities.
- Disclosing, using, or disseminating personal information regarding students.
- Cyber bullying, hate mail, defamation, harassment of any kind, discriminatory jokes and remarks and other unauthorized uses as referenced in WVBE policies or other policies and laws.
- Personal gain, commercial solicitation and compensation of any kind.
- Any activity which results in liability or cost incurred by the district.
- Downloading, installing and/or executing non-educational gaming, audio files, video files or other applications (including shareware or freeware) without permission or approval.
- Support or opposition for ballot measures, candidates and any other political activity.
- Information posted, sent or stored online that could endanger others (e.g., bomb construction, drug manufacture, etc.).
- Plagiarism or reproducing or repurposing audio/video without permission/consent.
- Attaching unauthorized equipment to the district or school networks. 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. Vandalism is defined as any attempt to harm or destroy data of another user or to intentionally damage equipment or any connections that are part of the Internet. This includes, but is not limited to, uploading, downloading or creating computer viruses. Vandalism will result in revocation of user privileges.
- Uses related to or in support of illegal activities will be reported to authorities.