EDUCATIONAL PURPOSE AND ACCEPTABLE USE OF ELECTRONIC RESOURCES, TECHNOLOGIES AND THE INTERNET

Policy Applies to: students, school personnel, volunteers, community members, parents, and guardians.

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.

The Summers County Board of Education concurs with the general goals outlined within *WVDE Policy 2460 Educational Purposes and Acceptable Use of Electronic Resources*, *Technologies and the Internet* and adopts the following to be followed on all Summers County Technology Recourses including but not limited to County and State Internet and Intranet, County purchased Software, Hardware, Cloud Based Services, and Software as Web Services.

Purpose:

This policy is intended to meet local, state and federal statutes and regulations pertaining to safe and acceptable use of the Internet, various digital resources and technologies, compliance with E-rate guidelines, and reinforcement of copyright compliance.

Educational Purposes:

To help prepare students who are globally aware, engaged with their communities, and capable of managing their lives and careers to succeed in a digital world.

Educators should integrate technology 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.

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.

Outline consequences for violation of safety and acceptable use in alignment with federal and state laws, state and district policies, specifically W. Va. 126CSR99, WVBE Policy 4373, Expected Behavior in Safe and Supportive Schools (Policy 4373) Employee and Student Handbook(s) in addition to the Student Discipline Referral Guidelines.

Digital Citizenship:

The appropriate use of technology and digital resources promotes positive and effective digital citizenship among students and staff. 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.

All users need to be part of this digital citizenry to appropriately and safely learn, work, play, and live in today's global society.

The International Society for Technology in Education (ISTE) includes standards and provides guidance related to digital citizenship for students, teachers, administrators, instructional coaches and computer science educators.

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. Faculty and staff are prohibited from using removable / portable storage devices and or media for storage and or transportation of student identifiable data. 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 the use of the state provided Microsoft One-Drive account is recommended.

Educators electing to use third party classroom based applications must request approval from the Summers County School Office of Technology prior to implementation. 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. Any technology utilized that is publicly viewable (blogs, web publishing, vlogs and so on) must receive parental permission and be actively moderated by the instructor. 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 Policy 4350, Procedures for the Collection, Maintenance and Disclosure of Student Data (Policy 4350).

Activate the appropriate automatic reply message 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.

Notify the appropriate school authority of any dangerous or inappropriate information or messages encountered.

Security:

Users (student and staff) who identify a security problem on any Summers County Board of Education managed system (internet, intranet, software, learning management, third party services) must notify the system administrator. Users who are aware of or suspect that confidential information may have been exposed to unauthorized parties must notify district and/or state officials responsible for implementing privacy incident response protocol consistent with federal and state regulations including, but not limited

to, Policy 4350 and the Student Data Accessibility, Transparency, and Accountability Act, W. Va. Code §18-2-5h.

Users must not demonstrate security problems to users other than school or county administration.

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, county, or school policies.

Any user identified as a security risk may be denied access by the appropriate disciplinary authority and or system administrator.

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.

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, W. Va. Code § 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 Summers County Board of Education's Internet and Telecommunications Access Consent and Waiver Form. It is also the educator's responsibility to refrain from using 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.

Students will be provided equitable access to technology.

The Summers County Board of Education reserves the right to monitor, inspect, investigate, copy, review, and store, without prior notice, information about the content and usage of any network and system files, user files, disk space utilization, applications, bandwidth utilization, document files, folders, electronic communications, e-mail, Internet access, and any and all information transmitted or received in connection with networks, e-mail use, and web-based tools.

The Summers County Board of Education and approved service providers will support local, state, and federal investigations as required by law. The WVDE and Summers County Board of Education reserves

the right to disclose any electronic message, files, media, etc., to law enforcement officials or third parties as appropriate.

The Summers County Board of Education reserves the right to enter an employee's information system files whenever there is a business need to do so.

Electronic filtering will be installed by the WVDE at the two points of presence (POPs) for Internet access. This will provide filtering for all public schools in a cost effective manner and with efficient management. Providing this service at the state level enables districts/schools to meet Children's Internet Protection Act (CIPA) and E-rate-guideline requirements for filtering. The Summers County Board of Education maintains a web filtering list in addition to the WVDE. The Summers County Board of Education reserves the right to block, limit, throttle, and monitor web usage at it discretion.

The Summers County Board of Education will not be responsible for unauthorized financial obligations resulting from the use of, or access to, the state's computer network or the Internet.

The Summers County Board of Education makes no warranties of any kind, whether expressed or implied, for the service being provided. The WVDE will not be responsible for any damages, including loss of data or service interruptions. The use of any information obtained via the system is at the user's own risk.

The Summers County Board of Education may provide students (including those enrolled in adult basic education), teachers, parents, and citizens access to technology in the public schools during non-school hours and in accordance with E-rate guidelines and network security best practices.

Professional development in the use of technology and its application in the teaching and learning process will be provided by the Summers County Board of Education.

Districts, schools, educators, and staff may publish student pictures, video images or names on class, school or district web sites and social media only when such elements are designated by district policy as directory information in accordance with FERPA and Policy 4350. Parental consent/permission should be obtained (e.g., through photo release forms).

District equipment is subject to existing rules and policies whether onsite or offsite.

Students and staff are expected to use district technology in a responsible, efficient, ethical, and legal manner in accordance with the educational mission of the district and school. The use of such technologies may be restricted or revoked for inappropriate behavior or use.

The use of student personal devices (e.g. cell phones, smart phones, tablets, digital cameras, MP3 players, and laptops) will not be supported on the Summers County School network and should not be utilized in the educational environment. Student personal devices should be powered off and out of sight during school hours.

The Summers County Board of Education may permit Faculty and Staff use of personal cell phones and or smart devices on the county network pursuant to Summers County Board of Education guidelines. Faculty and Staff personal devices will not receive technology support beyond local wireless connection. Faculty and Staff personal devices must be named in a way the devices can be easily identified on the network. By connecting a device to the Summers County LAN the Faculty and Staff member agrees to follow all items contained within this policy and will have no expectation of privacy.

Unauthorized or unacceptable use of personal technology devices may result in suspension or revocation of personal device privileges. These uses include, but are not limited to, the following:

Using personal devices to gain or give an advantage in a testing situation.

Using unapproved personal devices during class.

Downloading and installing district licensed software on personal devices unless specifically allowed by the licensing agreement.

Using personal devices to bypass filtering, circumvent network security, or in violation of the acceptable use standards which normally apply to district-owned technology.

Using personal devices for violations related to cyber bullying and harassment.

It is the responsibility of the student, parent, teacher, and administrator to follow acceptable use policies, as well as state and federal laws, so that access to telecommunication networks, computers and the Internet provided by the school, district, and state educational systems is not abused.

The viewing, storing, transmitting, or downloading of pornography or sexually suggestive or sexually explicit material or text on a work provided computer or other work provided electronic storage or communication device or service, whether at home or at work, by school personnel or anyone else to whom the school personnel has made the computer or other electronic storage or communication device available, is prohibited. This same prohibition applies to a personal computer or other electronic storage or communication device while at school or a school activity.

All information stored within work computers or servers is the property of the state, district or school, and the personnel using such computers/servers/networks have no expectation of privacy with respect to its contents.

Educators will promote and model acceptable use, digital citizenship and online responsibility to support personalized learning and digital-age assessments to meet applicable educational learning policies, for all students.

Teachers, specialists, and other supervising adults will teach and discuss the appropriate use of electronic resources, technologies and the Internet with their students, monitor their use, and intervene if the uses are not acceptable.

School personnel who receive information via any electronic resource, including a social networking site, that falls under the mandatory reporting requirements of W. Va. Code §49-2-803, must report as law requires.

Staff members shall not use materials in violation of copyright law or contrary to terms of use provided by the owner of the materials. Summers County Schools assumes no liability for local violations of copyright law.

School personnel are responsible for protecting their passwords associated with their computers and e-mail address and must not make them accessible to others.

Use of Electronic Resources, Technology and the Internet.

Unauthorized, unacceptable, or unsafe use of the Internet as part of an educational program by students, educators or staff may result in suspension or revocation of access privileges.

Each student accessing 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 school.

The WVDE provides the network system, e-mail accounts, and Internet access as tools for education and administration in support of the WVBE's and Summers County Schools' mission. Users have no expectation of privacy. The WVDE and Summers County Schools 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 Summers County Board of Education 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 student or staff use an Internet account not specifically created for him or her. Based upon the acceptable use and safety guidelines outlined in this document, the WVDE, State Superintendent of Schools, WVDE system administrators, and the Summers County Board of Education will determine what is appropriate use, 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 be found in Policy 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. Summers County Board of Education reserves the right to access data maintained in or transmitted over county 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. The Summers County Board of Education reserves the right to enter an employee's information system files whenever there is a legitimate 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.

Acceptable Use:

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 Summers County Board of Education. 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 districts and schools.

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, district, and school, to implement the intent of CIPA, COPPA, E-rate guidelines, FERPA, and any other applicable state and federal statute and policy, including but not limited to Policy 4373 and W. Va. Code §18-2C-3.

Acceptable network use by students and staff includes, but may not be limited to the following:

1. Creation of files, projects, and various media products using-network resources in support of student personalized learning and educational administration.
2. Appropriate participation in school-sponsored sites and online groups.
3. 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.
4. Incidental personal use by staff not contrary to district/school policies and guidelines.

Unacceptable Use:

1. 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.
2. Use for commercial activities by for-profit institutions is not acceptable.
3. Use for product advertisement or political lobbying is also prohibited.
4. 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:

1. Viewing, creating, accessing, uploading, downloading, storing, sending, or distributing obscene, pornographic, or sexually explicit material.
2. 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.
3. 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.
4. 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.
5. Supplying your password to others.
6. Storing passwords in a file without encryption.
7. Using the "remember password" feature of Internet browsers and e-mail clients.
8. Leaving the computer without locking the screen or logging off.
9. Corrupting, destroying, deleting, or manipulating system data with malicious intent.
10. Requesting that inappropriate material be transferred.
11. Violating safety and/or security measures when using any form of electronic communications.
12. Hacking, cracking, vandalizing, or any other unlawful online activities.
13. Disclosing, using, or disseminating personal information regarding students.
14. Cyber bullying, sending 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.
15. Personal gain, commercial solicitation, and compensation of any kind.
16. Any activity which may result in liability or cost incurred by the district.
17. Unauthorized downloading, copying, installing and/or executing gaming, audio files, video files or other applications (including shareware or freeware).
18. 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.
19. Posting, sending, or storing information that could threaten or endanger others.
20. Engaging in plagiarism or reproducing/repurposing media without permission.
21. Attaching unauthorized equipment to the district or school networks or network connected devices. Any such equipment may be confiscated and/or turned over to law enforcement officers for potentially violating W. Va. Code §61-3C-5.
22. Attaching unauthorized equipment or making unauthorized changes to the **County** network. Unauthorized equipment may be confiscated and/or turned over to law enforcement officers for potentially violating W. Va. Code §–61-3C-5. Only WVDE network personnel may authorize changes affecting the state backbone network.
23. 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.
24. Uses related to or in support of illegal activities.
25. Provision of 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.

26. Extending the County network to any device.
27. Creating a network not maintained, supported and filtered by the Summers County Board of Education.

Network.

The statewide network, the district wide area networks (WANs), and school local area networks (LANs) include wired and wireless computers, peripheral equipment, routers, switches, servers, files, storage devices, e-mail, Internet content, digital tools, and any other equipment which communicates via network connections.

Summers County Schools reserves the right to prioritize the use of and access to the statewide network. Summers County Board of Education may also prioritize local traffic within WANs and LANs consistent with WVDE guidelines.

All use of the network must support instructional and administrative purposes and be consistent with Summers County Schools policies, WVDE policies and guidelines, E-rate regulations, and federal and state statutes.

WVDE, approved service providers, and other state agencies operate the statewide infrastructure to provide Internet access for all schools under the supervision of the WVBE. In accordance with state purchasing guidelines, filtering will be installed at the state network level at the two points of presence (POPs) for Internet access. This will provide filtering for all public schools in a cost effective manner and with efficient management. Providing this service at the state level enables districts to meet CIPA and E-rate guideline requirements for filtering.

Summers County Schools may also add additional electronic filters at the local network levels. Other objectionable material may be filtered. The determination of what constitutes "other objectionable" material is at the discretion of Summers County Schools Board of Education.

Schools must enforce the use of the filtering or electronic technical protection measures during any use of the network and computers/devices to access the Internet.

To avoid duplication of effort at the district/school levels, the WVDE will provide a method and instructional modules that allow districts/schools to certify compliance with the current FCC regulations regarding Internet safety policies.

Filtering.

Appropriate filtering must be maintained to meet E-rate guidelines. Because filtering software is not 100% effective, every user must take responsibility for his or her use of the network and Internet and avoid objectionable sites.

Safety and Acceptable Use of the Internet by Students and Educators

Any attempts to defeat or bypass the State and or County Internet filter or conceal Internet activity are prohibited. This includes, but is not limited to, proxies, https, special ports, modifications to browser settings, and any other techniques designed to evade filtering or enable inappropriate content.

E-mail inconsistent with the educational missions of the state, district, or school will be considered SPAM and blocked from entering e-mail boxes.

Appropriate adult supervision of Internet use must be provided. The first line of defense in controlling access by students to inappropriate material on the Internet is deliberate and consistent monitoring of student access and use of equipment.

Staff must make a reasonable effort to become familiar with the Internet and to monitor, instruct, and assist effectively in filtering and acceptable use issues.

Copyright.

Copyright laws protect the rights of people who create intellectual property by providing the creator with exclusive rights to license, sell, or use the works. A creator owns the rights of reproduction, adaptation, distribution, public performance, public display, digital transmission, and moral rights. Violation of copyright laws may expose the user, district, or school to legal action and/or financial penalties.

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. Consult the Fair Use Doctrine of the United States Copyright Act, (17 U.S.C. §101-810), for guidance about using such material in an educational context.

To discourage violation of copyright laws, the following compliance requirements are specified:

1. Employees and students are expected to adhere to the copyright laws.
2. Appropriate software licenses will be obtained for use in a network server system or other multi-access use.
3. Programs available through the statewide provisions of technology implementation must comply with stipulations of the various purchase agreements.
4. Unauthorized duplication of copyrighted material and/or use of such unauthorized material on state, district, or school equipment or networks is prohibited.
5. Students are to be taught the ethical and practical implications and consequences of plagiarism and software/media piracy.
6. Employees will be provided yearly reminders of their responsibility through a district chosen procedure to adhere to and enforce the copyright laws and will be provided in-service training if necessary.
7. Educators and students should perform due diligence by reviewing user agreements including, but not limited to, terms and conditions, terms of use, End User License Agreements (EULA), and copyright prior to utilizing content from resources and software licenses to ensure compliance with the terms of the user agreements.

8. Under federal law, employees violating copyright laws may be subject to fines, confiscation of material, and other prosecution. Violations may also result in the employee's suspension and/or dismissal.

Web Publishing.

Any and all publicly accessible websites and recourses shall be governed and maintained by the Summers County Central Board Office or designee.

1. Appropriate permission must be obtained for student web pages published within the West Virginia public K-12 intranet and from a public K-12 site to the Internet.
2. Helping a community organization develop a web site could be a learning experience/project for students. However, housing a community web site on a school/district server will take K-12 bandwidth and may violate E-rate or other regulations.

Web site content should:

1. Be appropriate, in good taste, and not harmful to any individual or group.
2. Follow FERPA, state, district, and school regulations when using student pictures and names. Parental permission should be obtained, and districts/schools must respect parental refusals. Internet guidelines stress the importance of not publishing personally identifiable information of students.
3. Comply with WVBE and Summers County Board of Education policies and regulations.
4. Include information such as an e-mail address of the responsible contact person, copyright, and the last date updated.
5. Remain current, be accurate, and incorporate easy and user-friendly navigation through the site.
6. Restrict business/commercial links or the acknowledgment of a business on a school/district web site to business partners and/or materials that are educational, provide technical support, or are germane to the educational mission of the school/district. Advertising commercial offerings is prohibited.
7. Comply with copyright, intellectual property, state, and federal statutes (specifically COPPA and CIPA) and international law.
8. Include the permission granted statement for all copyrighted materials.
9. Complies with all W3C and ADA standards.

Severability.

If any provision of this rule or the application thereof to any person or circumstance is held invalid, such invalidity shall not affect other provisions or applications of this rule.