ACCEPTABLE USE OF ELECTRONIC RESOURCES, TECHNOLOGIES AND THE INTERNET

Background

This policy is proposed to bring Pleasants County School District in compliance with West Virginia Department of Education Policy 2460 – Educational Purpose and Acceptable Use of Electronic Resources, Technologies and the Internet and the Children's Internet Protection Act (CIPA).

Purpose

The Pleasants County Board of Education recognizes that an effective public education system develops students who are globally aware, civically engaged, and capable of managing their lives and careers. The Board also believes that students need to be proficient users of information, media, and technology to succeed in a digital world.

Therefore, Pleasants County School District will use electronic resources as a powerful and compelling means for students to learn core subjects and applied skills in relevant and rigorous ways. It is the district's goal to provide students with rich and ample opportunities to use technology for important purposes in schools just as individuals in workplaces and other real-life settings. The district's technology will enable educators and students to communicate, learn, share, collaborate and create, to think and solve problems, to manage their work, and to take ownership of their lives.

The Board directs the Superintendent or designee to create strong electronic educational systems that support innovative teaching and learning, to provide appropriate staff development opportunities and to develop procedures to support this policy.

Procedure

These procedures are written to support the Electronic Resources, Technologies and the Internet Policy of the West Virginia Board of Education and to promote 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. 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. Expectations for student and staff behavior online are no different than face-to-face interactions.

All staff and students are required to abide by this policy and by WV BOE Policy 2460 – *Educational Purpose and Acceptable Use of Electronic Resources, Technologies and the Internet*. Signed agreements are required for all employees and students. Employee supervisors shall annually review technology acceptable use with employees under their supervision and require each employee to sign the Employee Technology Acceptable Use Agreement each year. The agreements are to be kept on file by the immediate supervisor. A procedure for ensuring annual review of technology acceptable use with all students will be implemented yearly by schools/principals. A Student Technology Access Consent and Waiver Agreement must be signed by the student and parent/guardian whenever a student first enrolls at a school. A new signed agreement is required whenever a student transfers or is promoted to a different school. Schools may develop additional acceptable use measures that exceed provisions of state and district policies, provided that such measures are printed on Technology Access Consent and Waiver Agreement. Whenever present, such additional measures are considered part of the agreement for that school.

Network

The district network includes wired and wireless computers and peripheral equipment, files and storage, e-mail and Internet content (blogs, web sites, web mail, groups, wikis, social media, networking, etc.). The district reserves the right to prioritize the use of, and access to, the network.

All use of the network must support education and research and be consistent with the mission of the district.

Acceptable network use by district students and staff includes:

- Creation of files, projects, videos, web pages and podcasts using network resources in support of educational research;
- Participation in blogs, wikis, bulletin boards, social networking sites and groups and the creation of content for podcasts, e-mail and web pages that support educational research;
- 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 policies and guidelines;
- Connection of any personal electronic device is subject to all guidelines in this document.

Unacceptable network use by district students and staff includes but is not limited to:

- Personal gain, commercial solicitation and compensation of any kind;
- Disclosing any confidential records without adequate authority to do so;
- Downloading, installation and use of unauthorized and/or non-educational games, audio files, video files or other applications (including shareware or freeware) without permission or approval from the school principal or technology staff;
- Support or opposition for ballot measures, candidates and any other political activity;
- Hacking, cracking, vandalizing, the introduction of viruses, worms, Trojan horses, time bombs and changes to hardware, software, and monitoring tools;
- Any attempt to disable or overload any computer system or to circumvent any system intended to protect the privacy or security of another user;
- Unauthorized access to other district computers, networks and information systems;
- Bullying, hate mail, defamation, harassment of any kind, discriminatory jokes and remarks, or any other use of school equipment to threaten, harass, or insult another person in violation of West Virginia Code § 18-2C-2. Emphasis is added as it pertains to race, color, religion, national origin, gender, sexual orientation, or disability;
- Information posted, sent or stored online that could endanger others (e.g., bomb construction, drug manufacture);
- Accessing, uploading, downloading, storage and distribution of violent, obscene, pornographic or sexually explicit material; and
- Attaching unauthorized equipment to the district network. Any such equipment will be confiscated and destroyed.
- Unauthorized disclosure use, or dissemination of personal information regarding yourself (if student) or of any student.
- Using social media to engage in non-professional interaction between employees and students in an inappropriate manner, as set forth in WVDE Policy 2460, Section 5.8.
- All other prohibited activities as listed in WVDE Policy 2460, Section 6.3.

The district will not be responsible for any damages suffered by any user, including but not limited to, loss of data resulting from delays, non-deliveries, mis-deliveries or service interruptions caused by its own negligence or any other errors or omissions. The district will not be responsible for unauthorized financial obligations resulting from the use of, or access to, the district's computer network or the Internet.

Internet Safety: Personal Information and Inappropriate Content

Students and staff should not reveal personal information, including a home address and phone number, on web sites, blogs, podcasts, videos, social media, wikis, e-mail or as content on any other electronic medium. Students and staff should not reveal personal information about another individual on any electronic medium. No student pictures with names can be published on any class, school or district web site unless the appropriate permission has

been granted in accordance with district policy 8.4: Procedures for the Collection, Maintenance, and Disclosure of Student Records. If students encounter dangerous or inappropriate information or messages, they should notify the appropriate school authority.

Internet Safety: Instruction
The school district will educate all students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response All schools/principals will monitor and ensure that these requirements are being implemented and followed.

Filtering and Monitoring
Filtering software is used to block or filter access to visual depictions that are obscene and all child pornography in accordance with the Children's Internet Protection Act (CIPA). Other objectionable material could be filtered. The determination of what constitutes "other objectionable" material is a local decision.

- Filtering software is not 100% effective. While filters make it more difficult for objectionable material to be received or accessed; filters are not a solution in themselves. Every user must take responsibility for his or her use of the network and Internet and avoid objectionable sites;
- Any attempts to defeat or bypass the district's Internet filter or conceal Internet activity are prohibited: unauthorized virtual private networks (VPNs), proxies, https, special ports, modifications to district browser settings and any other techniques designed to evade filtering or enable the publication of inappropriate content;
- E-mail inconsistent with the educational and research mission of the district will be considered SPAM and blocked from entering district e-mail boxes;
- The district will provide appropriate adult supervision of Internet use. The first line of defense in controlling access by minors to inappropriate material on the Internet is deliberate and consistent monitoring of student access to district computers;
- Staff members who supervise students, control electronic equipment or have occasion to observe student use of said equipment online, must make a reasonable effort to monitor the use of this equipment to assure that student use conforms to the mission and goals of the district; and
- Staff must make a reasonable effort to become familiar with the Internet and to monitor, instruct and assist effectively.

The WVDE and West Virginia Network for Educational Telecomputing (WVNET) operate the statewide infrastructure to provide access for all Pre-K-12 public schools. In accordance with state purchasing guidelines, filtering will be installed at the state level for Internet access. This will provide filtering for all public schools in a cost effective manner and with efficient management. The Pleasants County School District and/or schools may also add other electronic filters.

Copyright
Downloading, copying, duplicating and distributing software, music, sound files, movies, images or other copyrighted materials without the specific written permission of the copyright owner is generally prohibited. However, the duplication and distribution of materials for educational purposes are permitted when such duplication and distribution fall within the Fair Use Doctrine of the United States Copyright Law (Title 17, USC) and content is cited appropriately.

Web Publishing
Pleasants County Schools recognizes the educational benefits of publishing information on the Internet by school personnel and students. It also recognizes the importance of having guidelines that address content, overall responsibility, potential contributors, quality, technical standards and student protection. In addressing these issues, it will be the policy of the Pleasants County Board of Education to follow the "Web Publishing Guidelines" as set forth in WVDE Policy 2460 - Educational Purpose and Acceptable Use of Electronic Resources,

Technologies and the Internet.

Network Security and Privacy
Passwords are the first level of security for a user account. System logins and accounts are to be used only by the authorized owner of the account, for authorized district purposes. Students and staff are responsible for all activity on their account and must not share their account password.

These procedures are designed to safeguard network user accounts:

- Change passwords according to district policy;
- Do not use another user's account;
- Do not insert passwords into e-mail or other communications;
- If you write down your account password, keep it out of sight;
- Do not store passwords in a file without encryption;
- Do not use the "remember password" feature of Internet browsers; and
- Lock the screen, or log off, if leaving the computer.

Student Data is Confidential
District staff must maintain the confidentiality of student data in accordance with the Family Education Rights and Privacy Act (FERPA).

No Expectation of Privacy
The district provides the network system, e-mail and Internet access as a tool for education and research in support of the district's mission. The district reserves the right to monitor, inspect, copy, review and store, without prior notice, information about the content and usage of:

- The network;
- 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 network and e-mail use.

No student or staff user should have any expectation of privacy when using the district's network. The district reserves the right to disclose any electronic message to law enforcement officials or third parties as appropriate and in compliance with all applicable laws, rules and policies.

Disciplinary Action
All users of the district's electronic resources are required to comply with the district's policy and procedures and agree to abide by the provisions set forth in the district's Technology Access Consent and Waiver Agreement.

Violation of any of the conditions of use explained in the Technology Access Consent and Waiver Agreement, Acceptable Use of Electronic Resources, Technologies and the Internet Policy or in these procedures could be cause for disciplinary action, including suspension or expulsion from school and suspension or revocation of network and computer access privileges. Students will be disciplined for violations in accordance with West Virginia BOE Policy 2460, and employee violations will be addressed in accordance with the Employee Code of Conduct and, if necessary, West Virginia Code § 18A-2-8.

References:
West Virginia Board of Education Policy 2460
Children's Internet Protection Act (CIPA)

Children's Online Privacy Protection Act (COPPA)

Amended: June 7, 2012

Revised: May 28, 2015

Revised: February 9, 2017

PLEASANTS COUNTY SCHOOLS

Student Technology Access Consent and Waiver

Student Name_____(print)

To the parent(s) or guardian(s) of the above named student:

The purpose of technology in Pleasants County Schools is to support learning and enhance instruction. It is the general policy of Pleasants County Schools that all technology resources are to be used in a responsible, efficient, ethical and legal manner. Today's global network provides valuable educational content but also the availability of material that may not be considered appropriate or of educational value. Both West Virginia State Policy 2460 and Pleasants County Schools guidelines are established to ensure appropriate use.

USE OF THE INTERNET AND ONLINE SERVICES IS A PRIVILEGE NOT A RIGHT!

The student and his/her parent(s) or guardian(s) must understand that student access to any network is being developed to support the school system's educational mission. Pleasants County Schools makes no warranties with respect to network services and specifically assumes no responsibilities for:

1. The content of any advice received by a student from a source outside the Pleasants County School System;
2. Any costs, liability or damages caused by the way the student chooses to use his/her network access;
3. Any consequences of service interruptions or changes, even if these disruptions arise from circumstances under the control of the Pleasants County School System;
4. The privacy of electronic mail, which cannot be guaranteed.

As a technology user, I will adhere to all West Virginia State and Pleasants County Schools policies including the following acceptable use guidelines. It is the responsibility of the individual user to follow these guidelines with all technology equipment provided by Pleasants County Schools.

- I will not damage or interfere with the normal operation of any computer or network hardware or software;
- I will not interfere with or disrupt network users, services, traffic, or equipment. (Disruptions include, but are not limited to: DOS/DDOS attacks, distribution of unsolicited advertising, propagation of computer viruses, and using a network to make unauthorized entry to any other machine accessible via a network);
- I will respect system security and not attempt to bypass it. This includes, but is not limited to, "hacking" and attempting to interfere with system security software, and I recognize that doing so will result in immediate loss of Internet and/or online service privileges;
- I will only access programs and equipment I am authorized to use. I will not attempt to modify programs. I will refrain from any "gaming" except use of educational games that have been assigned and are supervised;
- I will not download, upload or install any software or files onto any computer or other devices unless I have the approval of the building network administrator or other authorized Pleasants County Schools personnel;
- I understand that these guidelines include use of personal devices such as notebook computers, cell phones, PDAs, MP3 players, handheld gaming systems and other electronic technologies. I will not access school network resources with such devices without the specific permission of the school technology staff. I will not use such devices for cheating, taking inappropriate pictures, copying of materials that could be used for cheating, text messaging, or any inappropriate communication;
- I will use only files I have created or files I am authorized to use; therefore, I will not change, copy, rename, delete, view or otherwise access files unless I have prior permission from the creator or technology staff;
- I will use only my assigned user name(s) and password(s). I will not share these or any other system passwords and will notify the technology staff of any security problems of which I am aware;
- I will limit my use of telecommunications in school to the educational objectives established by my teacher(s) and under the supervision of my teacher(s). I understand technology use may be monitored;
- I will not access telecommunications resources from outside sources such as cellular data plans or nearby residential/commercial

wireless access points;

- I will not attempt to bypass internet content filtering through the use of any personal or web proxy;
- I will not use telecommunications access provided by Pleasants County Schools for illegal purposes of any kind;
- I will not use telecommunications access to transmit threatening, obscene, or harassing materials;
- I will follow the rules of network etiquette, which include the use of appropriate language and polite responses;
- I will not use abusive language of any type, including swearing and name-calling;
- I will not divulge my home address, phone number, and personal information with another user for any purpose;
- I understand that information received online is private property, unless specified;
- I will not plagiarize information received in any form;
- I understand I may access email at school only through an approved Pleasants County Schools mail account and only for educational purposes. The "Office365 k12.wv.us" is an approved account. I may not access email at school through a free or unsecured email server, misrepresent myself, or use of an alias;
- I will not participate in direct electronic communications such as but not limited to text messaging, social media, message boards and web logs, chat rooms, and instant messaging unless assigned for a specific educational purpose and under the direct supervision of teacher(s) responsible for the assigned activity.

By signing this Consent and Waiver Form, I understand and agree that Pleasants County Schools will not be held responsible if I participate in inappropriate activities listed above. I understand my responsibility as a user of technology. I have read the above rules and realize that any infraction will cancel my user privileges and may result in further disciplinary action, including suspension from school.

STUDENT
I have read the aforesaid Consent and Waiver Form for the use of technology in the classroom. I understand that this access is for educational purposes only and restricted to classroom assignments.

Student Name (please print)_____

Student (signature)_____Date_____

PARENT or GUARDIAN
As the parent (guardian) of_____(student name), I have read the aforesaid Consent and Waiver Form for use of technology and have discussed this with my son/daughter. I understand that the school may assist my child in creating an account on an online site whose purpose is further the schools educational mission. I understand that this access is provided for educational purposes only and that it is the responsibility of my child to restrict his/her use to the classroom projects and/or activities assigned by the teacher. I also accept full responsibility for supervision if and when my child's use of technology is in a setting other than school. I also understand that the teacher cannot be held responsible for intentional infractions of the above rules by my son/daughter.

Parent/Guardian Name (please print)_____

Parent/Guardian (signature)_____Date_____

PLEASANTS COUNTY SCHOOLS

Staff Technology Access Consent and Waiver

Pleasants County Schools (PCS) encourages the use of technology to further its educational mission and to facilitate effective educational practices. It is the general policy of PCS that all technology resources are to be used in a responsible, efficient, ethical and legal manner. Both West Virginia State Policy 2460 and PCS guidelines are established to ensure safe and appropriate use.

As a technology user, I will adhere to all West Virginia State and PCS policies including the following acceptable use guidelines:

- **I understand that all students must have training annually and have a signed Technology Use Consent Form on file.**
- **I will sign, adhere to, and will enforce the PCS Student Technology Access Consent and Waiver Form, this Staff Technology Access Consent and Waiver, and Board Policy 7029 Acceptable Use of Electronic Resources, Technologies and the Internet.**
- I understand all students must be directly supervised when using technology resources.
- I understand that I must (with the help of the Media Specialist/TIS/other PCS designee) educate students about appropriate online behavior, including cyber bullying awareness and response and interacting with others when online (chats, wikis, blogs, social networking, etc.) I will provide on-going information to students about safe and acceptable use of technology.
- I will not share any of my assigned USERID's and/or passwords with anyone, nor will I allow **anyone** access to the network using my USERID and password. I will notify the system administrator of any security problems of which I am aware.
- I will use only appropriate language and polite responses and will not access, read, print, create, or send unethical, illegal, immoral, inappropriate, obscene, harassing materials or information of any type or use abusive language. I will not send or post information that might be misconstrued as representing the school's or the county's point-of-view.
- I will directly supervise any classroom activity (social networking, chat, wikis, blogs, etc.) using electronic messaging/posting and the activity will have a specific curricular purpose.
- I will not use bandwidth intensive resources unless I have the approval of the technology department or other authorized PCS personnel. This includes but is not limited to internet radio, continuous downloading, or streaming video.
- I will refrain from any "gaming" and other non-educational uses of technology. I will not permit students to access games except those educational games that are assigned and directly supervised.
- I will respect network security and not attempt to bypass it. This includes, but is not limited to, "hacking" and attempting to interfere with system security software. If I am aware network resources are being used inappropriately or bypassed, I will report it to the principal and authorized PCS personnel.
- I will treat all equipment with care and respect. On equipment assigned to me that does not receive network updates, I will keep antivirus and anti-spyware software current.
- Personal or county owned electronic devices should not interfere or disrupt the duties assigned to any employee. Most social networking sites are blocked from K12 network due to federal regulations. Therefore, personal devices should not be used during the school day to circumvent this.

In order to protect your professional reputation, PCS recommends that you do not accept students as friends on your personal social networking sites. Allowing students access to your social network, gives them the ability to download and share your information/photos with others.

Here are some other tips to help protect your professional reputation:

- Exercise caution when posting information on your social networking site.
- Do not discuss students or coworkers on your social network site.
- Do not post images that include students or coworkers on your personal site.

The technology user is personally responsible for his/her actions in accessing and utilizing the PCS's computer resources. Based upon the severity of the violation, inappropriate use of the computers, disciplinary action will be taken. In the case of vandalism or malicious destruction of data or equipment, user should expect to pay for all cost incurred in repair and/or replacement of damages.

I have read and understand the above rules and agree to comply with stated rules as they apply to the use of all personal or PCS technology in any PCS facility or at any event sponsored by PCS. By using PCS telecommunications, I have agreed to this policy.

Employee Name (Print)	Employee Signature	Date