COMPUTER, NETWORK, ELECTRONIC COMMUNICATIONS AND INTERNET ACCEPTABLE USE POLICY

Section I: Purpose

This policy helps students, employees and guests ("Users") understand acceptable use of the District's computer network and equipment, including, but not limited to, District-issued laptop computers, tablets, and all devices logged into the District's computer network, Internet, and electronic communications used during and after regular school/work hours.

Any District-owned technology used during the school/work day or used off District property shall be considered part of the Pen Argyl District Network and Electronic Communications System (PANS), which includes Internet access, whether wired, wireless, virtual, cloud, or by any other means. Guidelines for acceptable use during school/work hours extend to use of District technology after school/work hours and/or all use of The District's network from off-campus sites at any time through remote login procedures.

In accordance with Pen Argyl Area School District (PAASD) goals and policy, the Board supports the use of the Internet and other computer networks in the District's instructional program in order to facilitate learning and teaching through interpersonal communications, access to information, research, and collaboration. The use of the network facilities shall be consistent with and enhance the curriculum adopted by the School District as well as the varied instructional needs, learning styles, abilities, and developmental levels of students.

For Users, the School District's PANS systems must be used for Educational Purposes and performance of School District job duties. Incidental Personal Use (as defined in this Policy_ of School District computers is permitted for employees. Students may only use the PANS systems for educational purposes. PANS systems may include School District computers which are located or installed on School District property, at School District events, connected to the School District's network and/or systems, or when using its mobile computing equipment, telecommunication facilities in unprotected areas or environments, directly from home, or indirectly through another Internet service provider ("ISP"), and, if relevant, when Users bring and use their own personal computers or personal electronic devices, and, if relevant, when Users bring and use another entity's computer or electronic devices to a School District location, event, or connect it to a School District network.

If Users bring personal computers, or at the same time, personal technology devices brought onto the District's property, or at District events, or connected to the District's network, that the District reasonably believes contain District information or contain information that violates a District policy, or contain information/data that the District reasonably believes involves a criminal activity, they may be legally confiscated and referred to law enforcement authorities to ensure compliance with this Policy, other district policies, and to comply with the law. Nothing in this Policy is intended to prevent or discourage staff members from using their own personal computers or other personal technology devices at home in order to connect with the District's network for uses in conformance with this policy.

Users may not use their personal computers to access the District's intranet, Internet or any other PANS system unless approved by the Technology Department or designee, and/or authorized as part of the District's services for Users.

The School District intends to strictly protect its PANS systems against numerous outside and internal risks and vulnerabilities. Users are important and critical players in protecting these School District assets and in lessening the risks that can destroy these important and critical assets. Consequently, Users are required to fully comply with this Policy and to report immediately any violations or suspicious activities to the Assistant Superintendent. Conduct otherwise will result in actions further described in the Consequences for Inappropriate, Unauthorized and Illegal Use section found in the last section of this Policy and provided in other relevant School District policies, regulations, rules and procedures.

Section II: Definitions

Child Pornography – Under federal law, any Visual Depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where:

a. The production of such Visual Depiction involves the use of a minor engaging in sexually-explicit conduct.
b. Such Visual Depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually-explicit conduct.
c. Such Visual Depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually-explicit conduct. 18 U.S.C. § 2256, 20 U.S.C. § 6777, 47 U.S.C. § 254.

Under Pennsylvania law, any person who intentionally views or knowingly possesses or controls any book, magazine, pamphlet, slide, photograph, film, videotape, computer depiction or other

material depicting a child under the age of eighteen (18) years engaging in a prohibited Sexual Act or in the simulation of such Act. 18 Pa. C.S.A. § 6312, 24 P.S. § 4603.

Computer - Includes any School District owned, leased or licensed or User-owned personal hardware, software, or other technology device used on School District premises or at School District events, or connected to the School District network, containing School District programs or School District or student data (including images, files, and other information) attached or connected to, installed in, or otherwise used in connection with a Computer. For example, Computer includes, but is not limited to, the School District's and Users' desktop, notebook, chromebooks, tablet PC, iPad, Kindle, eBook readers, or laptop Computers, printers, facsimile machine, cables, modems, and other peripherals, specialized electronic equipment used for students' special educational purposes, Global Positioning System (GPS) equipment RFID, personal digital assistants (PDAs), iPods, MP3 players, thumbdrives, cell phones (with or without Internet access and/or recording and/or camera/video and other capabilities and configuration), telephones, mobile phones, or wireless devices, two-way radios/telephones, beepers, paging devices, laser pointers and attachments, Pulse Pens, and any other such technology developed. 20 U.S.C. § 6777, 18 U.S.C. § 2256.

Electronic Communications Systems – any messaging, collaboration, publishing, broadcast, or distribution system that depends on Electronic Communications resources to create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, or print electronic records for purposes of communication across electronic Communications network systems between or among individuals or groups, that is either explicitly denoted as a system for Electronic Communications or is implicitly used for such purposes. Further, an Electronic Communications system means any wire, radio, electromagnetic, photo optical or photo electronic facilities for the transmission/transfer of signs, signals, writings, images, sounds, data, or intelligence of any nature, wire or electronic Communications, and any computer facilities or related electronic equipment for the electronic storage or such communications. Examples include, but are not limited to, the internet, intranet, electronic mail services, voice mail services, tweeting, text messaging, instant messaging, GPS, PDAs, facsimile machines, cell phones (with or without Internet access and/or electronic mail and/or recording devices, cameras/video, and other capabilities and configurations).

Educational Purpose - Includes use of the Pen Argyl District Network and Electronic Communications System (PANS) for classroom activities, professional or career development, and to support the School District's curriculum, policies, regulations, rules, procedures, and mission statement.

Guest – includes, but is not limited to, visitors, workshop attendees, volunteers, independent contractors, adult education staff, students, performers, vendors, and consultants.

Inappropriate Matter – Includes, but is not limited to, visual, graphic, video, text and any other form of indecent, obscene, pornographic, child pornographic, or other material that is harmful to minors, sexually explicit, or sexually suggestive. Examples include, taking, disseminating, transferring, or sharing obscene, pornographic, lewd, or otherwise illegal images or photographs, whether by electronic data transfer or otherwise (such as sexting, e-mailing, texting, among others). Others include, hateful, illegal, defamatory, lewd, vulgar, profane, rude, inflammatory, threatening, harassing, discriminatory (as it pertains to race, color, religion, national origin, gender, marital status, age, sexual orientation, political beliefs, receipt of financial aid, or disability), violent, bullying, flagging, terroristic material, and advocating the destruction of property.

Incidental Personal Use - Incidental personal use of school Computers is permitted for employees so long as such use does not interfere with the employee's job duties and performance, with system operations, or with other system Users. Personal use must comply with this Policy, all other applicable School District policies, rules, regulations, rules, and procedures, as well as Internet Service Provider (ISP) terms, local, state and federal laws, and must not damage the School District's PANS systems.

Minor – for purposes of compliance with the federal Children's Internet Protection Act ("FedCIPA"), an individual who has not yet attained the age of seventeen (17) years. For other purposes, Minor shall mean the age of minority as defined in the relevant law. 18 U.S.C. § 2256, 20 U.S.C. § 6777, 47 U.S.C. § 254, 18 Pa. C.S.A. § 2903.

Obscene – under federal law, analysis of the material meets the following elements:

a. Whether the average person, applying contemporary community standards, would find that the material, taken as a whole, appeals to the prurient interest.

b. Whether the work depicts or describes, in a patently offensive way, sexual conduct specifically designed by the applicable state or federal law to be Obscene.

c. Whether the work taken as a whole lacks serious literary, artistic, political, educational, or scientific value.

20 U.S.C. § 6777, 42 U.S.C. § 254.

Under Pennsylvania law, analysis of the material meets the following elements:

a. The average person, applying contemporary community standards, would find that the subject material, taken as a whole, appeals to the prurient interest.

b. The subject matter depicts or describes in a patently offensive way, Sexual Conduct described in the law to be Obscene.
c. The subject matter, taken as a whole, lacks serious literary, artistic, political, educational or scientific value.

24 P.S. § 4603, 18 Pa. C.S.A. § 5903.

Sexual Act and Sexual Contact – as defined at 18 U.S.C. § 2246(2), at 18 U.S.C. § 2246 (3), and 18 Pa. C.S.A. § 5903.

Technology Protection Measures – a specific technology that blocks or filters Internet access to Visual Depictions that are Obscene, Child Pornography or Harmful to Minors. 24 P.S. § 4606.

Visual Depictions – includes undeveloped film and videotape and data stored on computer disk or by electronic means which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format but does not include mere words. 18 U.S.C. § 2256, 18 U.S.C. §1460.

Harmful to Minors – under federal law, any picture, image, graphic image file or other Visual Depictions that:

a. Taken as a whole, with respect to Minors, appeals to the prurient interest in nudity, sex, or excretion,

b. Depicts, describes, or represents in a patently offensive way with respect to what is suitable for Minors, an actual or simulated Sexual Act or Sexual Content, actual or simulated normal or perverted Sexual Acts, or lewd exhibition of the genitals, and

c. Taken as a whole lacks serious literary, artistic, political, educational or scientific value as to Minors.

Under Pennsylvania law, that quality of any depiction or representation in whatever form, of

nudity, sexual conduct, sexual excitement, or sadomasochistic abuse, when it:

a. Predominantly appeals to the prurient, shameful, or morbid interest of Minors.

b. Is patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable for Minors.

c. Taken as a whole, lacks serious literary, artistic, political, educational or scientific value for Minors. 20 U.S.C. § 6777, 47 U.S.C. § 254.

Section III: Authority

The Pen Argyl Area School District reserves the right to determine which network services will be provided through School District resources. It reserves the right to view and monitor all applications provided through the network, including email, to log Internet and network use, and to monitor fileserver space utilization by students and staff.

The Board establishes that use of the Internet is a privilege, not a right. Inappropriate, unauthorized, and illegal use may result in cancellation or suspension of those privileges and appropriate disciplinary action. The District will cooperate to the extent legally required with the ISP, local, state and federal officials in any investigation concerning or related to the misuse of the District's network, including copyright, security, and vandalism of District resources or equipment.

The Pen Argyl Area School District bears no responsibility for unauthorized charges or fees resulting from access to the Internet or information that is lost, damaged or unavailable due to technical problems.

USERS OF THE PEN ARGYL DISTRICT NETWORK AND ELECTRONIC COMMUNICATIONS SYSTEMS (PANS) SHOULD NOT HAVE AN EXPECTATION OF PRIVACY IN THE MATERIALS THAT ARE CREATED, SENT, STORED, OR RECEIVED BY THEM OR DISPLAYED ON OR OVER THE PANS, INCLUDING THEIR PERSONAL FILES. TO THE EXTEND ALLOWED BY LAWS AND REGULATIONS, PEN ARGYL AREA SCHOOL DISTRICT AUTHORIZED PERSONNEL MAY EXAMINE ALL MATERIAL STORED ON THE PEN ARGYL DISTRICT NETWORK AND ELECTRONIC COMMUNICATIONS SYSTEM WITHOUT PRIOR NOTICE AT ANY TIME AND FOR ANY REASON.

Electronic communication systems, including but not limited to messages that are created, sent, or received using PANS's e-mail system, are the property of the PAASD. The PAASD reserves the right to access and disclose the contents of all messages created, sent, or received using the e-mail system. The e-mail system is strictly for official PAASD messaging. All communications on The District's network are property of the Pen Argyl Area School District.

Subject to local laws and regulations, the PAASD may monitor any aspects of its computerized resources from any District owned electronic device, including, but not limited to, monitoring sites visited by users on the Internet, monitoring chat groups and newsgroups, reviewing material downloaded from or uploaded to the Internet by a PANS user, and reviewing e-mail sent and received by PANS users.

It is often necessary to access Users' accounts in order to perform routine maintenance and security tasks. System administrators have the right to access by interception and to access the stored communication of User accounts for any reason in order to uphold this Policy, other school district policies, regulations, rules, and procedures, the law, and to maintain the system. USERS SHOULD HAVE NO EXPECTATION OF PRIVACY IN ANYTHING THEY CREATE, STORE, SEND, RECEIVE, OR DISPLAY ON OR OVER THE PANS SYSTEMS, INCLUDING THEIR PERSONAL FILES OR ANY OF THEIR USE OF THE PANS SYSTEMS. The School District reserves the right to record, check, receive, monitor, track, log, access, and otherwise inspect any and all PANS systems use and to monitor and allocate fileserver space. Users of the PANS systems who transmit or receive communications and information shall be deemed to have consented to having the content of any such communications recorded, checked, received, monitored, tracked, logged, accessed and otherwise inspected or used by the School District, and to monitor and allocate fileserver space. Passwords and message delete functions do not restrict the School District's ability or right to access such communications or information.

The School District reserves the right to restrict access to any Internet sites or functions it may deem inappropriate through general policy, software blocking or online server blocking. Specifically, the School District operates and enforces Technology Protection Measures(s) that block or filter online activities of Minors on its computers used and accessible to adults and students so as to filter or block Inappropriate Matter as defined in this Policy on the Internet. Measures designed to restrict adults' and Minors' access to material Harmful to Minors may be disabled to enable an adult or student (who has provided written consent from a parent or guardian) to access bona fide research, not within the prohibitions of this Policy, or for another lawful purpose. No person may have access to material that is illegal under federal or state law. 20 U.S.C. § 6777, 17 U.S.C. § 512.

Expedited review and resolution of a claim that the Policy is denying a student or adult to access material will be enforced by an administrator, supervisor, or their designee, upon the receipt of a written consent from a parent or guardian for a student, and upon the written request from an adult presented to the Assistant Superintendent.

The School District has the right, but not the duty, to inspect, review or retain electronic Communications created, sent, displayed, received, or stored on or over its PANS systems, to monitor, record, check, track, log, access or otherwise inspect; and/or to report all aspects of its PANS systems use. This includes any User's personal Computers, network, Internet, Electronic Communication Systems, Computers, databases, files, software, and media that they bring onto School District property, or to School District events, that are connected to the School District network and/or systems, and/or that contains School District programs, or School District or other Users' data or information, all pursuant to the law, in order to ensure compliance with this Policy and other school district policies, regulations, rules, procedures, ISP terms, and local, state, and federal laws, to protect the School District's resources, and to comply with the law.

The School District reserves the right to restrict or limit usage of lower priority PANS systems and Computer uses when network and computing requirements exceed available capacity according to the following priorities:

a. Highest – uses that directly support the education of the students.

b. Medium – uses that indirectly benefit the education of the students.

c. Lowest – uses that include reasonable and limited educationally-related interpersonal communications, and limited personal use.

d. Forbidden – all activities in violation of this Policy, other school district regulations, rules, and procedures, ISP terms, and local state and federal laws.

The School District additionally reserves the right to:

a. Determine which PANS systems' services will be provided through School District resources.

b. Determine the types of files that may be stored on School District file servers and Computers.
c. View and monitor network traffic, file server space, processor, and system utilization, and all applications provided through the network and Electronic Communications Systems, including email and other Electronic communications.

d. Remove excess email and other Electronic Communications or files taking up an inordinate

amount of fileserver space after a reasonable time.

e. Revoke User privileges, remove User accounts, or refer to legal authorities and/or School District authorities when violation of this and any other applicable School District policies, regulations, rules, and procedures occur or ISP terms, or local, state or federal law is violated, including, but not limited to, those governing network use, copyright, security, privacy, employment, vendor access, data breaches, and destruction of School District resources and equipment.

4. Responsibility

Due to the nature of the Internet as a global network connecting billions of Computers around the world, Inappropriate Matter can be accessed through the network and Electronic Communications systems. Because of the nature of the technology that allows the Internet to operate, the District cannot completely block or filter access to these resources. Accessing these and similar types of resources may be considered an unacceptable use of School District resources and will result in actions explained further in the Consequences for Inappropriate, Unauthorized and Illegal Use section, found in the last section of this Policy, and as provided in other relevant School District policies, regulations, rules, and procedures. Part of the District's Internet safety policy includes educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyber bullying awareness and response.

Users must be capable and able to use the PANS systems and software relevant to their responsibilities. In addition, Users must practice proper etiquette, School District ethics, and agree to the requirements of this Policy, regulations, rules, and procedures.

Section IV: Delegation of Responsibility

The Assistant Superintendent and/or designee will serve as the coordinator to oversee the PANS systems and will work with other regional or state organizations as necessary to educate Users, approve activities, provide leadership for proper training for all Users in the use of the PANS systems and the requirements of this Policy, establish a system to insure adequate supervision of the PANS systems, maintain executed User PANS Acknowledgement and Consent forms, and interpret and enforce this Policy.

The Assistant Superintendent and/or designee will establish a process for setting up individual

and class accounts, set quotas for disk usage on the system, establish a Records Retention and Record Destruction Policies, and Records Retention Schedule to include electronically stored information, and establish the School District virus protection process.

Unless otherwise denied for cause, student access to the PANS systems resources shall be through supervision by the professional staff. Administrators, teachers and staff have the responsibility to work together to help students develop the skills and judgment required to make effective and appropriate use of the resources. All Users have the responsibility to respect the rights of all other Users within the School District and School District PANS systems, and to abide by the policies, regulations, rules and procedures established by the School District, its ISP terms and local, state and federal laws.
Section V: Guidelines

Student Privacy Rights And Employee Sites
All teachers and District employees must be aware that all personal and professional blogs and social networking communications, even when authored/utilized outside of the school day and off school grounds, are subject to FERPA and other student privacy laws, including those found in the IDEA. Dissemination of private student information over these sites is expressly prohibited by law and this policy. Student records may not be sent by e-mail or placed in the cloud environment, such as Google Docs, due to the Family Education Rights and Privacy Act and state confidentiality rules.

Students must be directly supervised in the use of the Internet and email by District staff.
The building administration, working in conjunction with the Superintendent and the technology department, shall have the authority to determine what is inappropriate use and the consequences for that inappropriate use.

School District Limitation Of Liability
The District makes no warranties of any kind, either expressed or implied, that the functions or the services provided by or through The District's computer network systems will be error-free or without defect. The District does not warrant the effectiveness of Internet filtering. The electronic information available to users does not imply endorsement of the content by The District. The District is neither responsible for nor guarantees the accuracy or quality of the information obtained through or stored on The District's computer network systems. The District shall not be responsible for any damage users may suffer, including but not limited to, information that may be lost, damaged, delayed, misdelivered, or unavailable when using the network and electronic communications systems. The District shall not be responsible for material that is retrieved through the Internet, or the consequences that may result from them. The District shall not be responsible for any unauthorized

financial obligations, charges or fees resulting from access to The District's computer network systems. In no event shall The District be liable to the user for any damages whether direct, indirect, special or consequential, arising out of the use of The District's computer network systems.
The District disclaims any and all liability for actions of booster clubs, school support groups and school-related organizations including, without limitation, the PTA, and individuals who use their own websites, Face Book pages, blogs, or other non-school social media to show photos of, or make comments about District students.

Use Of Non-District Internet Access During School Hours, On School Grounds Or At School Functions

The provisions of this policy shall also apply to student and employee use of the Internet and other network access not provided by The District, including personal Internet access through laptops, PDAs and other devices, when such access occurs during school hours, on school grounds, or at school functions and all use of The District's computer network systems at any time through the use of remote login procedures.

Procedures

Only the authorized owner of the account shall use network user accounts, on PANS, for its authorized purpose. Accounts will be made available according to a schedule developed by appropriate District authorities given the capability of District hardware. Accounts will be given out to only those individuals who meet the following requirements:

a. Have read the District Computer, Network, Electronic Communications and Internet Acceptable Use Policy and indicate their agreement with its provisions by signing the signature page and returning it to the appropriate District authority. Students must have a parent or guardian sign the signature page indicating the parent or guardian's agreement with the policy and his/her consent to allow the student to access and use the network.

b. Students and Staff must have successfully completed an annual District orientation course, which will include but not be limited to instruction on network access, use, acceptable vs. unacceptable uses, network etiquette, and the consequences of abuse of privileges and responsibilities.

c. Each school in the District shall provide an annual written notice to the parents/guardians

of students about The District Internet system, the policies governing its use, and the limitation of liability of The District. Parents/Guardians of students attending traditional or cyber school classes must sign an agreement to allow their child to access the Internet. Upon receipt of the executed agreement, the student will be issued an Internet username and password. The agreement and the Internet username will be effective for as long as the student is enrolled in

The District. Parents/Guardians have the right to request the termination of their child's Internet access at any time.

Network accounts shall be used only by the authorized owner of the account for its approved purpose. Network users shall respect the privacy of other users on the system.

Prohibitions

Students, employees, and guests are expected to act in a responsible, ethical and legal manner in accordance with District Policy, accepted rules of network etiquette, and federal and state law, the Code of Professional Practice and Ethics, and the Public School Code. Additionally, this expectation applies to employees when using school computers after work hours and when using the District's network at any time through the use of remote login procedures. Specifically, the following uses are prohibited, but not limited to:

1. Use of the network or District computers to facilitate illegal activity.

2. Communication focused on commercial or for-profit purposes.

3. Communication of private/personal information of others.

4. Participation in online gaming and/or gambling.

5. Product advertisement or political lobbying.

6. Hate mail, discriminatory remarks and offensive, inflammatory, or inappropriate communication.

7. Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials.

8. Access (send, receive, view, download, or transmit) sexually suggestive, sexually explicit, obscene or pornographic material or child pornography.

9. Access by students and minors to material that is harmful to minors or is determined inappropriate for minors in accordance with Board policy.

10. Use of inappropriate language or profanity.

11. Transmission of material likely to be offensive or objectionable to recipients.

12. Intentional retrieval or modification of files, passwords, and data belonging to other users.

13. Impersonation of another user or communicating anonymously.

14. Fraudulent copying/reproduction, communications, or modification of materials in violation of copyright laws.

15. Loading or use of unauthorized games, programs, files, or other electronic media.

16. Disruption of the work of other users.

17. Destruction, modification, abuse or unauthorized access to network hardware, software and files.

18. Quoting, summarization or other recounting of personal communications in a public forum without the original author's prior consent.

19. Cyberbullying or any other type of harassment prohibited by law, the Student Code of Conduct, or Board policy.

20. Using District technology for social networking, including chat rooms or email with students beyond the District educational program.

21. Staff members texting students for any reason other than for school-related communication.

22. Participation in online gambling.

<u>Consequences for Inappropriate, Unauthorized and Illegal Use</u>

General rules for behavior, ethics, and communications apply when using the Pen Argyl Network Communication Systems, in addition to the stipulations of this Policy, other School District policies, regulations, rules, and procedures, ISP terms, and local, state, and federal laws. Users must be aware that violations of this Policy or other School District policies, regulations, rules, and procedures or for unlawful use of the PANS, may result in loss of PANS access and a variety of other disciplinary actions including, but not limited to, warnings, usage restrictions, loss of privileges, position reassignment, oral or written reprimands, student suspensions, employee suspensions (with or without pay), dismissals, expulsions, breach of contract, and/or legal proceedings on a case-by-case basis. This Policy incorporates all other relevant School District policies, such as, but not limited to, the student and professional employee discipline policies, Code of Student Conduct, cell phone policy as stipulated in Student Handbook, copyright, property, curriculum, terroristic threat, and harassment policies.

Users are responsible for damages to computers, the network, equipment, electronic communications systems, and software resulting from accidental, negligent, deliberate, and willful acts. Users may also be responsible for incidental or unintended damage resulting from negligent, willful or deliberate violations of this Policy, other School District policies, regulations, rules, and procedures, ISP terms, and local, state, and federal laws. For example, users will be responsible for payments related to lost or stolen computers and/or School District equipment, and recovery and/or breach of the data contained on them.

Violations as described in this Policy, other School District policies, regulations, rules, and procedures may be reported to the School District and to appropriate legal authorities, whether the ISP, local, state, or federal law enforcement, and may constitute a crime under state and/or federal law which may result in arrest, criminal prosecution, and/or lifetime inclusion on a sexual offenders registry. The School District will cooperate to the extent legally required with authorities in all such investigations.

Vandalism will result in cancellation of access to the School District's PANS systems and resources and is subject to discipline. Vandalism is defined as any malicious attempt to harm or destroy data of another user, Internet or other networks; this includes but is not limited to uploading or creating computer viruses.

Any and all costs incurred by the School District for repairs and/or replacement of software, hardware, and data files and for technological consultant services due to any violation of this Policy, other School District policies, regulations, rules, and procedures, or ISP, local, state or federal law, must be paid by the User who causes the loss.

Responsibility for Lost or Damaged District Computers, Laptops, and Network Facilities

In all cases of destruction or damage to a laptop computer or tablet by students or staff, the building administrator shall investigate and decide whether the destruction or damage resulted from intentional or malicious conduct. The building administrator's decision in this regard shall be final. Parents and guardians or staff members may be responsible for the entire cost of the repair or replacement resulting from any destruction or damage of a laptop or tablet, whether intentional, malicious or accidental. Parents and guardians or staff members may be responsible for the entire cost where the laptop computer is lost or stolen. An annual insurance policy, with a deductible, will be available for student issued laptop computers or tablets.

The Technology Department of the Pen Argyl School District will complete repairs or have them completed in the most cost effective manner, and will charge for labor and replacement parts. Parents and guardians are advised to determine whether their homeowner or renter's coverage provides insurance policy for destruction or damage to a school laptop computer.

Security

System security is protected through the use of passwords. Failure to adequately protect or update passwords could result in unauthorized access to personal or District files. To protect the integrity of the system, the following guidelines shall be followed:

1. Employees, students, and guests shall not reveal their passwords to another individual.

2. Users are not to use a computer that has been logged in under another student's or employee's name.
3. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the network.

4. Unauthorized access, including hacking and logging into networks using another individual's username and password is strictly prohibited and will result in discipline and denial of privileges. Such unauthorized use may also result in criminal charges.

Employee Use Of Social Networking Media

While The District understands the value of current social networking tools, prohibits employees from developing virtual relationships with students through social networking tools beyond The District educational program. The use of District technology for social networking with students beyond The District program and outside of the requirements of this policy is prohibited.

All personal communications with students must be of a professional nature. Faculty/staff members must maintain strict professional boundaries of communication with students. Faculty/staff members are encouraged not to "friend" students, allow students access to the employee's non-public personal pages, or use social networking media to enter into communications with students. PAASD takes personal/professional boundary limits with students very seriously and will take disciplinary action against any faculty or staff member who violates this policy and/or who initiates or maintains inappropriate personal communications and/or a personal relationship with a student through any means, including social networking.

If an employee, student or guest creates a blog with their own resources, the employee, student, or guest may not violate the privacy rights of employees and students, may not use School District personal and private information/data, images and copyrighted material in their blog; and may not disrupt the School District.

The District requires that faculty and staff take all necessary steps to limit access to their personal social networking media and prevent students from obtaining such access. FACULTY/STAFF MEMBERS ARE REMINDED THAT, DUE TO THE NATURE OF THE TECHNOLOGY, INDIVIDUALS DO NOT HAVE AN EXPECTATION OF PRIVACY ON SOCIAL MEDIA SITES.

<u>Faculty/Staff Members May Not:</u>

1. Utilize personal social media sites to communicate with students for educational purposes;

2. Enter into inappropriate communications/relationships with students via personal social media websites or other electronic means;

3. Post or share on a public site or site to which students have access to information that discusses or portrays sex, nudity, alcohol or drug use or other behaviors associated with the staff member's private life that would be inappropriate to discuss with a student at school;

4. Post or share information about identifiable students on any site, personal or professional without prior parental written notification and written consent;

5. Disclose personally identifiable information about co-workers or supervisors on any site, personal or professional, without prior written permission;

6. Post or share discriminatory or defamatory information on any site, personal or professional;

7. Post or share comments personal or professional that would cause a disruption in the educational environment on any site;

8. Suggest in any personal social networking context that the employee/faculty member in any way represents The District or is speaking on behalf of The District; or

9. Violate any District Policy on a social media site, including The District's Policies on discrimination, harassment, privacy, bullying.

Copyright

The illegal use of copyrighted software by students and staff is prohibited. Any data uploaded to or downloaded from the network shall be subject to fair use guidelines. District guidelines on plagiarism, as well as the Student Code of Conduct, will govern the use of material accessed through The District network. The District's guidelines on plagiarism can be found in each school's student handbook. Teachers will instruct students in appropriate research and citation practices.

Internet Safety Programs

The District Administration shall assure students are educated regarding appropriate on-line behavior, including interacting with other individuals on social networking websites and in chat rooms and cyber-bullying awareness and response. Plans for educating students as set forth above shall be periodically reviewed and updated by the District Administration. Users of the District computer system who engage in bullying activities will be subject to discipline described in the Consequences for Inappropriate, Unauthorized, and Illegal Use section of this Policy.

It is the teacher's responsibility to provide clear guidelines, direction, and supervision for the use of all technologies with their students. It is also the staff's responsibility to protect the confidentiality of computer-accessible student information.