WYOMING AREA SCHOOL DISTRICT

SECTION: OPERATIONS

TITLE: ACCEPTABLE USE OF INTERNET, COMPUTERS AND NETWORK RESOURCES

ADOPTED: September 20, 1999

REVISED: June 19. 2012

	815. ACCEPTABLE USE OF INTERNET, COMPUTERS AND NETWORK RESOURCES
1. Purpose	The Board supports use of the computers, Internet and other network resources in the district's instructional and operational programs in order to facilitate learning, teaching and daily operations through interpersonal communications and access to information, research and collaboration. The district provides students, staff and other authorized individuals with access to the district's computers, electronic communication systems and network, which includes Internet access, whether wired or wireless, or by any other means. For instructional purposes, the use of network facilities shall be consistent with the curriculum adopted by the district as well as the varied instructional needs, learning styles, abilities, and developmental levels of students.
2. Definitions	**CIPA** – The Children's Internet Protection Act (CIPA) is a federal law enacted to address concerns about access to offensive content over the Internet on school and library computers. CIPA requirements include the following three items: 1. Technology Protection Measure – A technology protection measure is a specific technology that blocks or filters Internet access. It must protect against access by adults and minors to visual depictions that are obscene, child pornography, or – with respect to the use of computers with Internet access by minors – harmful to minors. It may be disabled for adults engaged in bona fide research or other lawful purposes. For schools, the policy must also include monitoring the online activities of minors. 2. Internet Safety Policy – The Internet safety policy must address, access by minors to inappropriate matter on the Internet, the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications, unauthorized access including "hacking" and other unlawful activities by minors online, unauthorized disclosure, use, and dissemination of personal information regarding minors, and measures designed to restrict minors' access to harmful materials.

	3. Public Notice and Hearing – The authority with responsibility for administration of the school or library must provide reasonable public notice and hold at least one public hearing to address a proposed technology protection measure and Internet safety policy. **Child** – The term child means an individual under the age of 13 defined in the Children's Online Privacy Protection Act of 1998 (COPPA). The term child pornography is defined under both federal and state law.
18 U.S.C. Sec. 2256	**Child pornography** - under federal law, is 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: 1. The production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; 2. 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; or 3. Such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.
18 Pa. C.S.A. Sec. 6312	**Child pornography** - under state law, is 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. **COPPA** – Children's Online Privacy Protection Act applies to the online collection of personal information by persons or entities under U.S. jurisdiction from children under 13 years of age. It details what a website operator must include in a privacy policy, when and how to seek verifiable consent from a parent or guardian, and what responsibilities and operator has to protect children's privacy and safety online including restrictions on the marketing to those under 13. **Educational purpose** – includes use of the information technology tools, network resources, and Internet access for classroom activities, professional or career development, and to support the school district's curriculum, policy and mission statement. **Hacking** – any attempt to gain unauthorized access (or the unauthorized access) to network resources or using district network resources to attempt or to gain unauthorized access to other networks or computing resources.

	The term harmful to minors is defined under both federal and state law.
20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254	**Harmful to minors** - under federal law, is any picture, image, graphic image file or other visual depiction that: 1. Taken as a whole, with respect to minors, appeals to a prurient interest in nudity, sex or excretion; 2. 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 contact, actual or simulated normal or perverted sexual acts, or lewd exhibition of the genitals; and 3. Taken as a whole lacks serious literary, artistic, political or scientific value as to minors
18 Pa. C.S.A. Sec. 5903	**Harmful to minors** - under state law, is any depiction or representation in whatever form, of nudity, sexual conduct, sexual excitement, or sadomasochistic abuse, when it: 1. Predominantly appeals to the prurient, shameful, or morbid interest of minors; 2. Is patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable for minors; and 3. Taken as a whole lacks serious literary, artistic, political, educational or scientific value for minors. **HIPPA –** Health Insurance Portability and Accountability Act, pertaining to the Privacy Rule for Protected Health Information. The Protected Health Information is any information about health status, provision of health care, or payment for health care that can be linked to a specific individual. **Illegal activities/uses –** any use of network resources which violates a municipal ordinance, or local, state, or federal law, including those activities relating to intellectual property rights, trade secrets, the distribution of obscene or pornographic materials or the Family Educational Rights and Privacy Act. **Information technology –** any electronic device, computer hardware and software, operating systems, web-based information and applications, telephones and other telecommunications products, video equipment and multimedia products, information kiosks and office products such as photocopiers and fax machines.

	Network resources – 1. Computer hardware and software, electronic connections, electronic devices and other information technology tools used for information processing, as well as peripheral devices connected to these tools. 2. Network bandwidth including Internet bandwidth and other devices necessary to facilitate network connectivity such as e-mail services, file servers, routers, switches, hubs, firewalls, premise wiring, network data ports, etc. 3. Computers hardware and software, electronic connections electronic devices and other information technology tools used on district property or used off district property that impacts the district or causes a disruption to the educational environment, or when such use comes in conflict with the Student Code of Conduct or district policy, whether or not such tools are owned by the district and whether or not they are connected physically or wirelessly to the district's information network(s). 4. Computers, electronic connections, electronic devices and other information technology tools while they are connected remotely (from home or elsewhere) to the district's network.
18 Pa. C.S.A. Sec. 5903	**Obscene** - any material or performance, if: 1. The average person applying contemporary community standards would find that the subject matter taken as a whole appeals to the prurient interest; 2. The subject matter depicts or describes in a patently offensive way, sexual conduct described in the law to be obscene; and 3. The subject matter, taken as a whole, lacks serious literary, artistic, political, educational or scientific value. **Online collaboration –** using site-based or web-based technology tools to communicate and work productively with other uses to complete educationally relevant tasks. **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. **Staff –** includes administrative, teaching, support and volunteer personnel employed by or voluntarily affiliated with the Wyoming Area School District.

47 U.S.C. Sec. 254	**Technology protection measure** - a specific technology that blocks or filters Internet access to visual depictions that are obscene, child pornography or harmful to minors.
3. Authority	The availability of access to electronic information does not imply endorsement by the district of the content, nor does the district guarantee the accuracy of information received. The district shall not be responsible for any information that may be lost, damaged or unavailable when using the network or for any information that is retrieved via the Internet.
Pol. 218,233,317	The Board declares that computer and network use is a privilege, not a right. The district's computer and network resources are the property of the district. Users shall have no expectation of privacy in anything they create, store, send, delete, receive or display on or over the district's Internet, computers or network resources, including personal files or any use of the district's Internet, computers or network resources. The district reserves the right to monitor, track, and log network access and use; monitor fileserver space utilization by district users; or deny access to prevent unauthorized, inappropriate or illegal activity and may revoke access privileges and/or administer appropriate disciplinary action. The district shall cooperate to the extent legally required with the Internet Service Provider (ISP), local, state and federal officials in any investigation concerning or related to the misuse of the district's Internet, computers and network resources. The Board requires all users to fully comply with this policy and to immediately report any violations or suspicious activities to the Superintendent or designee.
47 U.S.C. Sec. 254	The Board establishes the following materials, in addition to those stated in law and defined in this policy, that are inappropriate for access by minors: { } Defamatory. { } Lewd, vulgar, or profane. { } Threatening.
Pol. 103,103.1 104,248,348	{ } Harassing or discriminatory.
Pol. 249	{ } Bullying.
Pol. 218.2	{ } Terroristic. { } _____ (specify others).

24 P.S. Sec. 4604 20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254	The district reserves the right to restrict access to any Internet sites or functions it deems inappropriate through established Board policy, or the use of software and/or online server blocking. Specifically, the district operates and enforces a technology protection measure(s) that blocks or filters access to inappropriate matter by minors on its computers used and accessible to adults and students. The technology protection measure shall be enforced during use of computers with Internet access.
24 P.S. Sec. 4604	Upon request by students or staff, the Superintendent or designee shall expedite a review and may authorize the disabling of Internet blocking/filtering software to enable access to material that is blocked through technology protection measures but is not prohibited by this policy.
24 P.S. Sec. 4610 20 U.S.C. Sec. 6777	Upon request by students or staff, building administrators may authorize the temporary disabling of Internet blocking/filtering software to enable access for bona fide research or for other lawful purposes. Written permission from the parent/guardian is required prior to disabling Internet blocking/filtering software for a student's use. If a request for temporary disabling of Internet blocking/filtering software is denied, the requesting student or staff member may appeal the denial to the Superintendent or designee for expedited review.
4. Delegation of Responsibility	The district shall make every effort to ensure that this resource is used responsibly by students and staff.
24 P.S. Sec. 4604	The district shall inform staff, students, parents/guardians and other users about this policy through employee and student handbooks, posting on the district website, and by other appropriate methods. A copy of this policy shall be provided to parents/guardians, upon written request. Users of district networks or district-owned equipment shall, prior to being given access or being issued equipment, sign user agreements acknowledge awareness of the provisions of this policy, and awareness that the district uses monitoring systems to monitor and detect inappropriate use { } and tracking systems to track and recover lost or stolen equipment. Student user agreements shall also be signed by parent/guardian. Administrators, teachers and staff have a professional responsibility to work together to help students develop the intellectual skills necessary to discern among information sources, to identify information appropriate to their age and developmental levels, and to evaluate and use the information to meet their educational goals.

	Students, staff and other authorized individuals have the responsibility to respect and protect the rights of every other user in the district and on the Internet. Building administrators shall make initial determinations of whether inappropriate use has occurred.
20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254 47 CFR Sec. 54.520	The Superintendent or designee shall be responsible for recommending technology and developing procedures used to determine whether the district's computers are being used for purposes prohibited by law or for accessing sexually explicit materials. The procedures shall include but not limited to: 1. Utilizing a technology protection measure that blocks or filters Internet access for minors and adults to certain visual depictions that are obscene, child pornography, harmful to minors with respect to use by minors, or determined inappropriate for use by minors by the Board. 2. Maintaining and securing a usage log. 3. Monitoring online activities of minors.
47 U.S.C. Sec. 254 SC 1303.1-A Pol. 249	The Superintendent or designee shall develop and implement administrative regulations that ensure students are educated on network etiquette and other appropriate online behavior, including: 1. Interaction with other individuals on social networking websites and in chat rooms. 2. Cyberbullying awareness and response.
5. Guidelines	Network accounts shall be used only by the authorized owner of the account for its approved purpose. All communications and information accessible via the network should be assumed to be private property and shall not be disclosed. Network users shall respect the privacy of other users on the system. <u>Safety</u> It is the district's goal to protect users of the network from harassment and unwanted or unsolicited electronic communications. Any network user who receives threatening or unwelcome electronic communications or inadvertently visits or access an inappropriate site shall report such immediately to a teacher or administrator. Network users shall not reveal personal information to other users on the network, including chat rooms, email, social networking websites, etc.

47 U.S.C. Sec. 254 47 CFR Sec. 54.520	Internet safety measures shall effectively address the following: 1. Control of access by minors to inappropriate matter on the Internet and World Wide Web. 2. Safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications. 3. Prevention of unauthorized online access by minors, including "hacking" and other unlawful activities. 4. Unauthorized disclosure, use, and dissemination of personal information regarding minors. 5. Restriction of minor's access to materials harmful to them. <u>Prohibitions</u> Users 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. Specifically, the following uses are prohibited: 1. Facilitating illegal activity. 2. Commercial or for-profit purposes. 3. Nonwork or nonschool related work. 4. Product advertisement or political lobbying.
SC 1303.1-A Pol. 249	5. Bullying/Cyberbullying. 6. Hate mail, discriminatory remarks, and offensive or inflammatory communication. 7. Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials.
Pol. 237	8. Accessing, sending, receiving, transferring, viewing, sharing or downloading obscene, pornographic, lewd, or otherwise illegal materials, images or photographs. 9. Access by students and minors to material that is harmful to minors or is determined inappropriate for minors in accordance with Board policy.

Pol. 814	10. Inappropriate language or profanity. 11. Transmission of material likely to be offensive or objectionable to recipients. 12. Intentional obtaining or modifying of files, passwords, and data belonging to other users. 13. Impersonation of another user, anonymity, and pseudonyms. 14. Fraudulent copying, communications, or modification of materials in violation of copyright laws. 15. Loading or using 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. Accessing the Internet, district computers or other network resources without authorization. 19. Disabling or bypassing the Internet blocking/filtering software without authorization. 20. Accessing, sending, receiving, transferring, viewing, sharing or downloading confidential information without authorization. <u>Security</u> System security is protected through the use of passwords. Failure to adequately protect or update password could result in unauthorized access to personal or district files. To protect the integrity of the system, these guidelines shall be followed: 1. Employees and students 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 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.

	Copyright
17 U.S.C. Sec. 101 et seq Pol. 814	The illegal use of copyrighted materials is prohibited. Any data uploaded to or downloaded from the network shall be subject to fair use guidelines and applicable laws and regulations.
	District Website
	The district shall/may establish and maintain a website and shall develop and modify its web pages to present information about the district under the director of the Superintendent or designee. All users publishing content on the district website shall comply with this and other applicable district policies.
	Users shall not copy or download information from the district website and disseminate such information on unauthorized web pages without authorization from the building principal.
	Consequences For Inappropriate Use
24 P.S. Sec. 4604	The network user shall be responsible for damages to the equipment, systems, and software resulting from deliberate or willful acts.
	Illegal use of the network; intentional deletion or damage to files or data belonging to others; copyright violations; and theft of services shall be reported to the appropriate legal authorities for possible prosecution.
	General rules for behavior and communications apply when using the Internet, in addition to the stipulations of this policy.
	Vandalism shall result in loss of access privileges, disciplinary action, and/or legal proceedings. **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.
Pol. 218, 233, 317	Failure to comply with this policy or inappropriate use of the Internet, district network or computers shall result in usage restrictions, loss of access privileges, disciplinary action, and/or legal proceedings.

	References: School Code – 24 P.S. Sec. 1303.1-A PA Crimes Code – 18 Pa. C.S.A. Sec. 5903, 6312 Child Internet Protection Act – 24 P.S. Sec. 4601 et seq. U.S. Copyright Law – 17 U.S.C. Sec. 101 et seq. Sexual Exploitation and Other Abuse of Children – 18 U.S.C. Sec. 2256 Enhancing Education Through Technology Act – 20 U.S.C. Sec. 6777 Internet Safety, Children's Internet Protection Act – 47 U.S.C. Sec. 254 Children's Internet Protection Act Certifications, Title 47, Code of Federal Regulations – 47 CFR Sec. 54.520 Board Policy – 103, 103.1, 104, 218, 218.2, 220, 233, 237, 248, 249, 317, 248, 814