ALTOONA AREA SCHOOL DISTRICT

SECTION: OPERATIONS

TITLE: ACCEPTABLE USE OF INTERNET/INTRANET

ADOPTED: August 17, 2009

REVISED: April 18, 2010

815. ACCEPTABLE USE OF INTERNET/INTRANET

1. Purpose

The Board supports use of the Internet and other computer networks 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.

For instructional purposes, the use of network facilities shall be consistent with the curriculum adopted by the school district as well as the varied instructional needs, learning styles, abilities, and developmental levels of students.

2. Definition

Advanced Internet communication technologies refers, but not limited to, the latest generation of Internet development and design strategies, that facilitate improved communication, information sharing, and collaboration. These include the use of Internet based communities, hosted services, and applications such as social networking sites, video-sharing sites, wikis, blogs, texting, podcast, folksonomies, etc.

Network access/use is defined as access to network related infrastructure from within school district facilities using school district equipment, as well as any access to any district managed servers or other devices using personal/third party equipment locally or remotely.

3. Authority

The electronic information available to students and staff 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.

The district shall not be responsible for any unauthorized charges or fees resulting from access to the Internet.

The district reserves the right to log network use and to monitor fileserver space utilization by district users, while respecting the privacy rights of both district users and outside users.

	The Board establishes that network use is a privilege, not a right; inappropriate, unauthorized and illegal use will result in cancellation of those privileges and appropriate disciplinary action.
47 U.S.C. Sec. 254	The Board shall establish a list of materials, in addition to those stated in law, that are inappropriate for access by minors.
24 P.S. Sec. 4604	The Board shall designate an online server that blocks access to visual depictions of obscenity, child pornography, or material harmful to minors. Comments or actions utilizing advanced Internet communication technologies may be monitored. If deemed inappropriate for any reason, various actions may be taken by the district such as student discipline, deletion of inappropriate material, and possible legal recourse, if deemed necessary. The district must comply with federal regulations and mandates that apply to Children's Internet Protection Act (CIPA), Health Insurance Portability and Accountability Act (HIPAA), and Family Educational Rights and Privacy Act (FERPA).
4. Delegation of Responsibility	The district shall make every effort to ensure that this resource is used responsibly by students and staff. The district's computer network system operators, or other school official, may at any time review the subject, content and appropriateness of electronic communications or other computer files and remove them, if warranted, reporting any violation of rules to the school administration or law enforcement officials. Administrators, teachers and staff have a professional responsibility to work together to help students develop the intellectual skills necessary to discriminate 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 and staff have the responsibility to respect and protect the rights of every other user in the district and on the Internet. The building administrator shall have the authority to determine what is inappropriate use.

20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254	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 be 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.
24 P.S. Sec. 4604	The district shall provide a copy of this policy to parents/guardians, upon written request. Online communications using advanced Internet communication technologies such as blogging, texting, podcasting, and social networking sites offer students an instant, effective vehicle for student expression. The district takes student safety seriously and thus, expectations for blogging, student protected e-mail, podcast projects, or other web interactive use must follow established Internet/Intranet safety guidelines outlined in this policy.
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. When sending electronic messages or transmitting online registrations, staff members shall make every effort to prevent students from including information that could identify themselves or other students and staff without written consent from the parent/guardian and the instructor’s express permission. Examples of identifying information include last names, addresses, phone numbers, individual pictures, student ID’s, and passwords. ID’s and passwords, if supplied, are provided for the individual’s personal use. Do not share ID’s or passwords with anyone and do not use anyone else’s ID or password, regardless of how it was obtained. Users shall not intentionally seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users.

All students and their parents/guardians must annually sign acceptance of the *Internet/Intranet Acceptable Use Policy* prior to their being provided access to the Internet/Intranet by the district. This signed agreement shall be kept on file in the building where the student attends school.

All students and their parents/guardians must annually sign an *Internet/Intranet Publishing Release Form* if that student's work, picture and/or opinions are to be included on any of the Altoona Area School District's Web Sites or Altoona Area School District sponsored Internet/Intranet projects. This signed release form will be kept on file in the building where the student attends school.

Prohibitions

Students and staff 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.
8. Access to 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. 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 and/or use of anonymity or pseudonyms to perpetrate and/or attempt the perpetration of an otherwise prohibited act.

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. Quoting of personal communications in a public forum without the original author's prior consent.

The use of advanced Internet communication technologies may be considered an extension of a K-12 educational environment. Therefore, any speech that is considered inappropriate in a K-12 educational environment is also inappropriate when using advanced Internet communication technologies. This includes, but is not limited to, the guidelines expressed in this policy.

Students and staff using advanced Internet communication technologies are expected to act safely by keeping all personal information out of their posts. Students should never post personal information on the Internet including, but not limited to, last names, personal data including address or phone numbers, or photographs.

Do not agree to meet someone you have met over the Internet.

Never link to web sites from your blog or blog comment without reading the entire article to make sure it is appropriate for a K-12 educational environment.

Never share users name and passwords with anyone other than parents/guardians and appropriate district staff.

Speech that is inappropriate for a K-12 educational environment is also inappropriate for use when using any advanced Internet communication technologies.

	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 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'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. Consequences For Inappropriate Use 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 of data belonging to others, copyright violations, and theft of services will 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. Loss of access and other disciplinary actions shall be consequences for inappropriate use.
Pol. 218, 317	Vandalism will result in cancellation of access privileges. **Vandalism** as defined for this policy is any attempt to change or destroy data of another user, Internet/Intranet, or any other network that is connected to the Altoona Area School District networks. This includes, but is not limited to the uploading or creation of computer viruses. Staff members and/or students committing such vandalism shall be subject to discipline consistent with Board policy and the Student Code of Conduct. Copyright
Pol. 814	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.

	Safety To the greatest extent possible, users of the network will be protected from harassment and unwanted or unsolicited communication. Any network user who receives threatening or unwelcome communications 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, e-mail, Internet, etc.
20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254	Any district computer/server utilized by students and staff shall be equipped with Internet blocking/filtering software.
47 U.S.C. Sec. 254	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 minors' access to materials harmful to them. 6. Educating minors about appropriate online behavior, including interacting with other individuals on social networking web sites and in chat rooms and cyberbullying awareness and response.

	References: School Code – 24 P.S. Sec. 1303.1-A Child Internet Protection Act – 24 P.S. Sec. 4601 et seq. Enhancing Education Through Technology Act of 2001 – 20 U.S.C. Sec. 6777 Internet Safety – 47 U.S.C. Sec. 254 Board Policy – 218, 249, 317, 814 Student Internet/Intranet Acceptable Use Policy Internet/Intranet AUP Signature Form TEC-P006 (03_09) CIPA Compliance Procedure