Student Technology Acceptable Use/ Student Code of Conduct

School District of Altoona

The School District of Altoona continues to make a significant investment in technology and technology access. The Board supports access by students and staff to technology resources and wants to insure that students use technology efficiently and safely. Students who use the Districts' technology resources assume responsibility for their appropriate use. The District expects students to be careful, honest, and responsible in their use of school technology. The computers, software, and network resources are owned by the District and are provided to support students in meeting their educational goals. The information in this policy aligns with the guidelines for the Children's Internet Protection Act (CIPA) passed by Congress in December 2000.

With the approval of the staff member in charge, limited personal use of school district technology is permitted so long as the following conditions are met: personal use shall not be allowed when other users are in need of computers for educational work, shall not be used to play games unless assigned by a teacher with a clear and definable educational purpose, shall not violate any rules contained in any school district policy, or any state or Federal law, and shall not damage or alter the District's hardware, software or communications systems including use that degrades or disrupts network performance.

Personal use of district technology resources for commercial or political activities or for financial gain is prohibited. Computers shall not be used to view or disseminate sexually explicit, vulgar, indecent, obscene, offensive, lewd, or harassing communications to other individuals or organizations. Criminal sanctions are provided under Wis. Stat. 947.0125 for threatening, intimidating, abusive, or harassing messages sent to another person through electronic mail or other digital communication systems.

Students shall not intentionally seek password information, obtain copies of, or modify files, or other data, belonging to other users on the network. Students shall not disclose to online entities or organizations any personal identification information or other students while using district technology resources.

The District will not be held liable for information that may become lost, damaged, or unavailable due to technical or other difficulties. The District is not liable for losses, claims, or demands against the District or any user by any other party based on the user's unethical or illegal use of technology resources.

Internet and Electronic Communications Students using school computers may use only their school provided email account and will not enter any "Social networking sites" such as "MySpace.com unless instructed to by a teacher for a clear and definable educational purpose.

Network Storage Students are provided with file server storage space for the school year. At the end of each year file server space is cleared of all files.

Computer Hardware and Software Computer hardware and software are provided for students to be used in fulfilling their educational goals. Students shall not alter hardware or software configurations, download and/ or install software on any District owned equipment. All software that is installed on the district owned computers must, be legally licensed by the District.

Internet Safety Policy

Introduction It is the policy of the School District of Altoona to (a) prevent user access over its computer network to, or transmission of, inappropriate material via the Internet, electronic mail, or other forms of electronic communications; (b) prevent unauthorized and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (d) comply with the Children's Internet Protection Act (CIPA) [Pub. L. No 106-554 and 47 USC 254(h)].

Definitions CIPA definitions of terms:

TECHNOLOGY PROTECTION MEASURE. The term "technology protection measure" means a specific technology that blocks or filters Internet access to visual depictions that are:

1. OBSCENE, as that term is defined in section 1460 of title 18, United States Code;

2. CHILD PORNOGRAPHY, as that term is defined in section 2256 of title 18, United States Code; or

3. Harmful to minors.

HARMFUL TO MINORS. The term "harmful to minors" means any picture, image, graphic image file, or other visual depiction that:

1. Taken as a whole and 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 a lewd exhibition of the genitals; and

3. Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

SEXUAL ACT; SEXUAL CONTACT. The terms "sexual act" and "sexual contact" have the meanings given such terms in section 2246 of title 18, United States Code.

Access to Inappropriate Material/ Inappropriate Network Usage The District shall take reasonable steps to promote the safety and security of users accessing the District's computer network, however no filtering technology is 100% effective in blocking all obscene, or "harmful" sites. Technology protection measures, such as "Internet filters", shall be used to block access to inappropriate information from the Internet or other digital communications. Use of any technology that renders the filtering process ineffective shall not be used.

Technology protection measures may be temporarily disabled only for clear and definable educational purposes, such research or other lawful purposes. As required by the Children's Internet Protection Act, prevention of inappropriate network usage includes: (a) unauthorized access, including so-called "hacking," and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

Supervision and Monitoring It shall be the responsibility of all staff members School District of Altoona to supervise and monitor usage of the computer network and access to the Internet in accordance with this policy and the Children's Internet Protection Act. Instructional staff will provide developmentally appropriate instructional guidance to students as they use technology to support district curriculum.

The District reserves the right to inspect, review and remove any student mail and files from the server: such inspection may be conducted by school authorities deemed necessary, without notice, without student consent, and without a search warrant.

Users should consider all network activities public and not private. The District reserves the right to monitor, access and disclose a user's Internet activities and email content without notification or permission.

Discipline and Penalties Failure to follow appropriate practices may result in disciplinary action including loss of the individual's access to technology resources. Serious abuses may result in suspension or expulsion. When applicable, law enforcement agencies may be involved. After the loss of privileges, students will be required to apply for reinstatement. The administration will determine if the applicant will be reinstated. A parent or guardian must sign the application for reinstatement.

Summary of Student Acceptable Use of Technology

Expectations of Students	
Acceptable use includes:	**Unacceptable Uses include but are not limited to:**
Careful use of technology	Sending sexually explicit, vulgar, indecent, obscene, offensive, or lewd communications
Honesty	Harassing - including bullying, teasing, threats, or suggestive language or graphics
Responsibility	Using other students' accounts or sharing passwords
Use for educational purposes	Entering chat rooms or social networking site such as MySpace.com.
Deleting unneeded files and email	Playing games not assigned by a teacher
Personal-with approval of staff member in charge	Sharing personal identification information about self or other students
	Installing software on District computers
	Violating school rules, policies or Federal or state laws
	District Access to Student Files

This chart represents a summary of the Technology Acceptable Use policy. It is the responsibility of students and parents to read the policy in its entirety for more specific details regarding acceptable use of District-owned technology resources.

- Altoona School District has the right to inspect, review, and remove any mail or files without notice, consent, or search warrant
- Computer Hardware and Software
- Students shall not alter or damage equipment (hardware or software)

- Discipline and Penalties
- Computer privileges may be taken away
- Following the loss of privileges, student will need to reapply with a parent's signature
- Other disciplinary action may be taken

Initial Adoption: 09/ 18/ 95

Final Adoption: 10/ 02/ 95

Amended: 07/ 10/ 06