ACCEPTABLE, SAFE AND RESPONSIBLE USE OF TECHNOLOGY RESOURCES Policy 363.2
(Replaces IIBG)

The purpose of this policy is to provide guidelines for access to the School District of Altoona's technologies, use of personal and district-owned devices within the District, use of the District's network and the acceptable and safe use of the Internet, including electronic communications.

The School District of Altoona considers its own stated mission, goals, and objectives in making decisions regarding student, employee, parent and community access to the School District of Altoona technology system, resources, and the Internet. Electronic information research skills are now fundamental to preparation of citizens and future employees. Access to the school district technology system and to the Internet enables students and employees to explore thousands of libraries, databases, and other resources while exchanging messages with people around the world. The School District of Altoona expects that staff will blend thoughtful, applicable, and motivational use of the school district technology system and the Internet throughout the curriculum and will provide guidance and instruction to students in their use.

The school district technology system is the property of the School District of Altoona. At no time does the District relinquish its exclusive control of electronic technologies. Inappropriate use of District electronic technologies, including interfering with network functions and the standardization of technologies, may result in the limitation or revocation of access. The purpose of this system is more specific than providing students and employees with general access to the Internet. The school district technology system is for educational purposes and to conduct the business of the District only. Users are expected to use the technology system and the Internet access through the district system to further educational and personal goals consistent with the mission of the school district and school policies. Uses which might be acceptable on a user's private personal account on another system may not be acceptable on this limited-purpose network.

The use of the School District of Altoona system and access to use of the Internet is a privilege, not a right. Internet access can be used—inadvertently or, in some cases, purposefully—to facilitate inappropriate, harmful, deceptive, and even illegal activities and communications. Further, notwithstanding reasonable efforts at prevention, there is still a risk that a student may, at some time, be exposed to particular content or participate in particular activities or communications that the District would consider harmful, deceptive, or otherwise inappropriate, or that a parent or guardian may find objectionable.

Consistent with applicable federal laws, the School Board believes that the best approach to student Internet safety involves a combination of technology protection measures, monitoring, and instruction. The District's comprehensive approach to student internet safety shall take into account the differing ages and instructional levels of the students in the District.

It shall be the responsibility of the District's technology director and building principal in consultation with such designees as they deem appropriate, to:

- Ensure that the District's systems and equipment that provide access to the Internet make active use of technology protection measures designed to block or filter Internet access to visual depictions that are: (a) obscene; (b) pornographic; or (c) otherwise harmful to minors. Filtering, blocking or other protective technologies will also be used to decrease the likelihood that student users of the District systems and equipment might access materials or communications, other than visual depictions, that are inappropriate for students.

- Develop and implement procedures that provide for the monitoring of students' and other authorized users' activities when using District-provided equipment or District-provided network access or Internet access. Such monitoring may sometimes take the form of direct supervision of students' and minors' online activity by school personnel. School personnel has the right to randomly search District-provided equipment. To the extent consistent with applicable law, other examples of such monitoring activities may include the use of applications, services, equipment, or other methods by which school personnel can:

    - track and review users' Internet histories; online communications; other online activities, uploaded, downloaded, saved or deleted data, files, applications, programs or other content; or other online activities;

    - track and log network access and use by any person or under any account; or

    - monitor fileserver space utilization by District users by, for example, file size, file type, file content and/or file function.

- Develop and implement appropriate instruction to educate students about acceptable and responsible use of technology and safe and appropriate online behavior, including (a) safety and security issues that arise in connection with various forms of electronic communication; (b) information about interacting with other individuals on social networking sites and in chat rooms; and (c) cyberbullying awareness and response. Such technology safety instruction shall vary by the instructional level of the students and shall include (but shall not consist exclusively of) reinforcement of the provisions of the District's specific rules regarding student's acceptable and responsible use of technology while at school.

Building principals and their designees shall have responsibility, within their respective schools, for overseeing the day-to-day implementation of the District's policies, rules and guidelines regarding the acceptable, safe, and responsible use of technology resources.

Legal Reference: Wisconsin State Statute Sections: 120.12, 120.13, 120.18, 943.70, 947.0125

Federal Laws and Regulations: Children's Internet Protection Act (CIPA), Protecting Children in the 21st Century Act

ADOPTED: 10/02/95
AMENDED: 07/26/16