IJNDB ©
USE OF TECHNOLOGY RESOURCES IN INSTRUCTION

Appropriate use of Electronic Information Services

The District may provide electronic information services (EIS) to qualified students, teachers, and other personnel who attend or who are employed by the District. Electronic information services include networks (e.g., LAN, WAN, Internet), databases, cloud-based systems, and any computer-accessible source of information, whether from hard drives or other electronic sources. The use of the services shall be in support of education, research, and the educational goals of the District. To assure that the EIS is used in an appropriate manner and for the educational purposes intended, the District will require anyone who uses the EIS to follow its guidelines and procedures for appropriate use. Anyone who misuses, abuses, or chooses not to follow the EIS guidelines and procedures will be denied access to the District's EIS and may be subject to disciplinary and/or legal action.

The Superintendent shall determine steps, including the use of an Internet filtering mechanism, that must be taken to promote the safety and security of the use of the District's online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications. Technology protection measures shall protect against Internet access by both adults and minors to visual depictions that are obscene, child pornography or, with respect to use of computers by minors, harmful to minors. Safety and security mechanisms shall include online monitoring activities.

Inappropriate Use of Electronic Information Services

As required by the Children's Internet Protection Act and A.R.S. 15-120.05, the prevention of inappropriate network usage includes unauthorized access, including "hacking," and other unlawful activities; unauthorized disclosure, use and dissemination of personal identification information regarding minors; and student use of wireless communication devices.

It is the policy of the Board to:

A. prevent user access over the District's computer network, or transmissions of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications;

B. Limit the use of wireless communication devices and access to social media networks by students during the school day;

C. prevent unauthorized access and other unlawful online activity;

D. prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and

E. comply with the Children's Internet Protection Act [P.L. No. 106-554 and 47 U.S.C. 254(h)] and A.R.S. 15-120.05.

Each user will be required to sign an EIS user's agreement. The District may log the use of all systems and monitor all system utilization. Accounts may be closed and files may be deleted at any time. The District is not responsible for any service interruptions, changes, or consequences. The District reserves the right to establish rules and regulations as necessary for the efficient operation of the electronic information services.

The District does not assume liability for information retrieved via EIS, nor does it assume any liability for any information lost, damaged, or unavailable due to technical or other difficulties.

Generative Artificial Intelligence Programs

The proper use of Artificial Intelligence (AI) programs can be effective at enhancing student learning and can prepare students with the competencies and knowledge needed in the digital age. Its use should also be guided by responsible and ethical considerations, including mitigating bias, promoting transparency, and providing AI benefits to all students. Use of AI programs in the classroom should be approved by the site administrator or Superintendent, and teachers' instructions and expectations should guide the classroom use of AI. Teachers should include relevant lessons on correct and responsible use of AI, and students should be taught standards regarding plagiarism and source citation and should use these guidelines if AI is used for a school assignment. AI use should be guided and monitored by teachers and/or administrators and should align with the District's guidelines and policies, including any relevant student rules/responsibilities. AI resources should be available to all students, including those with disabilities and English language learners. Use of an AI system should comply with the Family Educational Rights and Privacy Act (FERPA) and should support data privacy and security.

Filtering and Internet Safety

As required by the Children's Internet Protection Act, the District shall provide for technology protection measures that protect against Internet access by both adults and minors to visual depictions that are obscene, child pornography, or, with respect to use of the computers by students, harmful to students. The protective measures shall also include monitoring the online activities of students.

Limits, controls, and prohibitions shall be placed on student:

A. Access to inappropriate matter.

B. Safety and security in direct electronic communications.

C. Unauthorized online access or activities.

D. Unauthorized disclosure, use and dissemination of personal information.

Education, Supervision and Monitoring

It shall be the responsibility of all District employees to be knowledgeable of the Board's policies and administrative guidelines and procedures. Further, it shall be the responsibility of all employees, to the extent prudent to an individual's assignment to educate, supervise, and monitor appropriate usage of the online computer network and access to the Internet in accordance with this policy, the Children's Internet Protection Act, the Protecting Children in the 21st Century Act, and A.R.S. 15-120.05.

The Superintendent shall provide for appropriate training for District employees and for students who use the District's computer network and have access to the Internet. Training provided shall be designed to promote the District's commitment to:

A. the standards and acceptable use of the District's network and Internet services as set forth in District policy;

B. student safety in regards to use of the Internet, appropriate behavior while using, but not limited to, such things as social media platforms, online opportunities and chat rooms; and cyberbullying awareness and response; and compliance with E-rate requirements of the Children's Internet Protection Act. Teachers are allowed to give students access to social media platforms to the extent necessary for educational purposes.

Wireless Communication Devices

Districts shall limit student use of wireless communication devices during the school day except if any of the following apply:

A. for educational purposes, as directed by the student's teacher.

B. during an emergency.

C. The student needs the student's wireless communication device because the student has a medical condition.

Procedures shall include guidelines for a student's parent to contact the student during the school day and for a student to contact the student's parent

during the school day.

While training will be subsequently provided to employees under this policy, the requirements of the policy are effective immediately. Employees will be held to strict compliance with the requirements of the policy and the accompanying regulation, regardless of whether training has been given.

The Superintendent is responsible for the implementation of this policy and for establishing and enforcing the District's electronic information services guidelines and procedures for appropriate technology protection measures (filters), monitoring, and use.

Notification

At the beginning of each school year, parents teachers and students will be notified of the policies regarding the use of technology and the Internet while at school. The District shall provide to parents, teachers and students a copy of the adopted policies and notify the parents, teachers and students of any changes to the policy.

Parents will also be notified of their ability to prohibit the student from the use of technology and the Internet while at school in which covered information may be shared with an operator pursuant to A.R.S. 15-1046. This does not apply to software or technology that is used for the daily operations or administration of a local education agency or Arizona Online instruction programs authorized pursuant to A.R.S. 15-808.

Definitions:

A. "School day" means periods of time when students are at school, including meals, passing periods and recess.

B. "Social media platform" means a website, computer application or other digital platform that is used for social networking and creating or exchanging virtual content.

C. "Wireless communication devices" includes personal devices and devices that are provided by the school.

Adopted: September 17, 2025

LEGAL REF.:
A.R.S.
13-2316
13-3506.01
13-3509
15-120.05
15-341
15-808
15-1046

34-501
34-502
20 U.S.C. 1232g, the Family Educational Rights and Privacy Act
20 U.S.C. 1232h, the Protection of Pupil Rights Amendment
20 U.S.C. 1400 *et seq*., Individuals with Disabilities Education Act
20 U.S.C. 6301 *et seq*., Every Student Succeeds Act of 2015
20 U.S.C. 9134, The Children's Internet Protection Act
47 U.S.C. 254, Communications Act of 1934 (The Children's Internet Protection Act)
16 CFR Part 312, Children's Online Privacy Protection Rule (COPPA)