

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, and any computer-accessible source of information, whether from hard drives, tapes, compact disks (CDs), floppy disks, 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.

As required by the Children's Internet Protection Act, 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.

It is the policy of the Board to:

- 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;
- prevent unauthorized access and other unlawful online activity;

- prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and
- comply with the Children's Internet Protection Act [P.L. No. 106-554 and 47USC 254(h)].

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.

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:

- Access to inappropriate matter.
- Safety and security in direct electronic communications.
- Unauthorized online access or activities.
- 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, and the Protecting Children in the 21st Century Act.

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:

- the standards and acceptable use of the District's network and Internet services as set forth in District policy;
- student safety in regards to use of the Internet, appropriate behavior while using, but not limited to, such things as social networking Web sites, online opportunities and chat rooms; and cyberbullying awareness and response; and compliance with E-rate requirements of the Children's Internet Protection Act.

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.

Adopted: July 11, 2012

LEGAL REF.: A.R.S. 13-2316

13-3506.01

13-3509

15-341

34-501

34-502

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)