TUCSON UNIFIED SCHOOL DISTRICT **GOVERNING BOARD POLICY**	**POLICY TITLE: Use of ~~Technology Resources~~ Electronic Information Systems in Instruction** **POLICY CODE: IJNDB**

Electronic Information Systems (EIS): Definition

Tucson Unified School District provides 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.

Acceptable Use of EIS

The use of the services shall be in support of education, research, and the educational goals of the District. These resources are made available with the support and supervision of parents, teachers, and support staff. This policy shall not be construed to limit the use of district email as provided in any employee agreements.

Consequences for Failure to Follow Acceptable Use of EIS

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 and abide by the policies and regulations of the District. Anyone who misuses, abuses, or chooses not to follow the EIS guidelines and procedures and District policies and regulations will be denied access to the District's EIS and may be subject to disciplinary and/or legal action

Internet Filtering and Online Monitoring

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.

Unauthorized Access

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

and Disclosure

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 245(h)]

EIS User Agreement

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.

Disclaimer

The District does not assume liability for information retrieved via EIS. While the District will take reasonable steps to retrieve lost data, it does not 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, Tucson Unified School District has a content filtering program system which places barriers to help prevent access to sites that are deemed inappropriate (obscene, child pornography or harmful to students) for our users.

Monitoring Student Online Activities

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 or

personal information.

However, students may still encounter material that is inappropriate or offensive. **It is the student's responsibility not to access this type of information.**

TUSD Employees Responsible for 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.

Employee and Student Training Required

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 regard 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; Cyber bullying awareness and response 47 U.S.C. 254(h)(5)(B)(iii); and
- Compliance with E-rate requirements of the Children's Internet Protection Act 47 U.S.C. 254(h)(5)(B)(iii).

Full Compliance Required With or Without Training

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 for establishing and enforcing the District's electronic information services guidelines and procedures for appropriate technology protection measures (filters), monitoring, and use.

Parent Notification

Parents will be notified of the policies regarding the use of technology and the Internet while at school. 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.

Adopted: October 10, 2006
Revised: July 2, 2012
Revised: Approved with title change for review and feedback April 10, 2018

LEGAL REF:

A.R.S. 13-2316 Computer Tampering penalties
13-3506.01 Prohibition on furnishing harmful items to minors
13-3509 Duty to Report
15-341 Board Powers & Duties
15-808 Online instruction
15-1046 Student data privacy; parent notification
34-501 Definitions--pornography, etc
34-502 Public school protections – student access to internet
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)

CROSS REF:

EJA Acceptable Use of Technology Resources;
EJC - Electronic Mail.