TUCSON UNIFIED SCHOOL DISTRICT **GOVERNING BOARD REGULATION**	**REGULATION TITLE:** **USE OF TECHNOLOGY RESOURCES IN INSTRUCTION** **(Safety and use of Electronic Information Services)**
	REGULATION CODE: IJNDB-R1

Safety and Use of Electronic Information Services

Use of the electronic information services (EIS) requires that the use of the resources be in accordance with the following guidelines and support the education, research, and educational goals of the District. Filtering, monitoring, and access controls shall be established to:

- Limit access by minors to inappropriate matter on the Internet and World Wide Web.
- Monitor the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications.
- Monitor for unauthorized access, including so-called "hacking," and other unlawful activities by minors online.
- Restrict access by minors to materials harmful to minors.

Content Filtering

A content filtering program or similar technology shall be used on the networked electronic information system (EIS) as well as on standalone computers capable of District authorized access to the Internet. The technology shall at a minimum limit access to obscene, profane, sexually oriented, harmful, or illegal materials. Should a District adult employee have a legitimate need to obtain information from an access-limited site, a request to unblock the site may be submitted to TUSD Proxy Issues.

Employee Responsibilities for Education, Supervision and Monitoring

It is the responsibility of all District employees to be knowledgeable of the Board's policy and administrative regulations and procedures related to the use of technology resources.

Employees are further responsible, to the extent prudent to an individual's assignment, to educate, supervise, and monitor student use of the District's online computer network use.

District, department, and school administrators shall provide

employees with appropriate in-servicing and assist employees with the implementation of Policy IJNDB.

Monitoring

As a means of providing safety and security in direct electronic communications and to prevent abuses to the appropriate use of electronic equipment, all computer access to the Internet through the District electronic information systems (EIS) or standalone connection shall be monitored periodically or randomly through in-use monitoring or review of usage logs.

Access Control

Individual access to the EIS shall be by authorization only. Designated personnel may provide authorization to students and staff who have completed and returned an electronic information services user agreement. The Superintendent and/or his/her designee may give authorization to other persons to use the EIS.

Acceptable Use for Students

Each student user of the EIS shall:

- Use the EIS to support personal educational objectives consistent with the educational goals and objectives of the School District.
- Agree not to submit, publish, display, or retrieve any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or illegal material.
- Use clear, concise, and appropriate language. Think about what you have to say and how you say it. Email doesn't show sarcasm or wit as well as you might think. Respect privacy (yours and everyone else's). Do not repost a message without the permission of the person who sent it.
- Don't share personal information.
- Not use instant-messaging software at school unless under the auspices of a class project. Electronic communications should at all times be polite and considerate, and must not interfere with school or homework.
- Abide by all copyright and trademark laws and regulations.
- Not reveal home addresses, personal phone numbers or personally identifiable data unless authorized to do so by designated school authorities.
- Understand that electronic mail or direct electronic communication is not private and may be read and

monitored by school employed persons.

- Not use the network in any way that would disrupt the use of the network by others.
- Not use the EIS for commercial purposes.
- Follow the District's code of conduct.
- Not attempt to harm, modify, add, or destroy software or hardware nor interfere with system security.
- Understand that inappropriate use may result in cancellation of permission to use the electronic information services (EIS) and appropriate disciplinary action up to and including expulsion.
- Consequences for inappropriate actions are determined by Student Rights and Responsibilities.

Acceptable Use for District Employees Working with Students

Each District employee working with students shall:

- Maintain supervision of students using the EIS.
- When supervising students, agree to directly log on to student activity monitoring software and supervise student account activity when allowing students to use District accounts.
- Take responsibility for assigned personal and District accounts, including password protection.
- Take all responsible precautions, including password maintenance and file and directory protection measures, to prevent the use of personal and District accounts and files by unauthorized persons.

Student Email

Students may check email during breaks or at home, but not during class unless instructed to do so. Email "chain letters" are prohibited. Students should not exchange email with people whom they do not know, unless for legitimate school-related business.

Games

Games are prohibited during the academic day unless under the auspices of a class project

Internet Access

Students must have adult supervision while online. Use of the Internet is restricted to appropriate educational activities. Although the network does have a content filter, TUSD makes no guarantee that it will block all inappropriate material. At home, parents are responsible for monitoring Internet use.

Printers

Care should be taken when printing to avoid wasting resources or printing unnecessary items.

Privacy

Students must respect the privacy of others and the integrity of the network by accessing only appropriate files. Students log on to the network using a personal username and may not share passwords. Students should use caution when sharing their email address with others and only for school-related business.

EIS User Agreement

Each user will be required to sign an EIS user agreement (IJNDB-E1 Electronic Information Services User Agreement). A user who violates the provisions of the agreement will be denied access to the information services and may be subject to disciplinary action. Accounts may be closed and files may be deleted at any time. The District is not responsible for any service interruptions, changes, or consequences.

Details of the user agreement shall be discussed with each potential user of the electronic information services. At the start of school, after students have reviewed the EIS agreement with appropriate staff members, students will be provided a paper copy of the EIS to take home for review with their parent or guardian. Parents/guardians will also sign the EIS, and return it to the school. Students will not be given access to the EIS until after receiving parent/guardian signature on the EIS. When the signed agreement is returned to the school, the user may be permitted use of EIS resources through school equipment.

Reviewed: October 13, 2006 (Friday Report)
Revised: August 20, 2018