

**IJNDB
USE OF TECHNOLOGY RESOURCES
IN INSTRUCTION**

(Appropriate Use of Electronic Resources)

The Grand Canyon Unified School District (GCUSD) Governing Board recognizes that an excellent and engaging public education system develops students who are globally aware, civically engaged, and capable of managing their lives and careers. The Board also believes that students need to be proficient, responsible and safe users of information, media, and technology to succeed in a digital world.

Therefore, the District will use electronic resources as a powerful and compelling means for students to learn core subjects and applied skills in relevant and rigorous ways. It is the District's goal to provide students with rich and ample opportunities to use technology for important purposes in schools just as individuals in workplaces and other real-life settings use those tools. The District's technology will enable educators and students to communicate, learn, share, collaborate and create; to think and solve problems; to manage their work; and to take ownership of their reputations and lives.

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 or designee 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:

- 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. prevent unauthorized access and other unlawful online activity;
- C. prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and
- D. comply with the Children's Internet Protection Act [P.L. No. 106-554 and 47 U.S.C. 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.

Network Use Agreement

Any student, staff member, or guest using the Internet from an Internet-capable computing device at Grand Canyon Unified School District will be required to sign a network user agreement before access is granted.

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, 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:

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

B. 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; 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 or designee 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.

Instruction

All students will be educated about appropriate online behavior, including, but not limited to, interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response.

The Grand Canyon Unified School District is committed to preparing every student for the global workplace, for college, and for personal success in the 21st century. As part of this commitment, access to the District's wireless network, including the Internet, shall be made available to students, employees, and members of the Board of Directors primarily for instructional and administrative purposes and in accordance with this and other GCUSD policies. Guest access may be granted to users who have received advance approval as noted in the procedures of this policy. All users of the District's wireless network and electronic resources must comply with all School District policies and procedures including Policy IJNDB; Use of Technology Resources in Instruction (Responsible Use of Electronic Resources). Limited personal use of the District's wireless network shall be permitted if the use:

A. imposes no tangible cost to the District;

B. does not unduly burden the District's network or electronic resources; or

C. has no adverse impact on a student's academic performance and learning environment, or an employee's work responsibilities and job performance.

Access to the District's network system is a privilege. All users shall be required to acknowledge receipt and understanding of District policies, procedures, and agreements governing use of network systems and electronic resources and must comply with them. Noncompliance with policies, procedures, or user agreements may result in suspension or termination of privileges and other disciplinary action consistent with District policies.

The Board permits the use of personal, mobile, computing devices for educational and operational purposes. Computing devices shall not be used in any way that disrupts or detracts from the educational process or school and work environments. The Board further permits personal computing devices for non-disruptive use during non-instructional and non-operational times in locations designated by the administration. The use of personal computing devices during school-related activities may be permitted in accordance with guidelines established by the District.

Students, staff, and guest users are responsible for the devices they bring to school, on school buses, and to school-sponsored events. The District shall not be liable for the loss, theft, damages or misuse of any electronic device brought to school, possessed/used during the school day, in/on District buildings, District property, District vehicles, or contracted vehicles, during transport to/from school, while attending school-sponsored activities during the school day, and/or any/all school-sponsored activities. The District will provide no technical support, troubleshooting, or repair for personally owned computing devices.

The District reserves the right to monitor, inspect, copy, and review a personally owned device or file when administration has a reasonable suspicion that a violation has occurred.

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, 2018

LEGAL

REF.:

A.R.S.

[13-2316](#)

[13-3506.01](#)

[13-3509](#)

[15-341](#)

[15-808](#)

[15-1046](#)

[34-501](#)

[34-502](#)

18 U.S.C. 2510-2522 Electronic Communication Privacy Act Protecting
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) and Authentication Policies
47 U.S.C. 254(1)(B) Children's Internet Protection Act
Pub. L. No. 106-554 Neighborhood Children's Internet Protect Act
Pub. L. No. 110-385 Protecting Children in the 21st Century Act