For purposes of this policy, “technology resources” means electronic communication systems and electronic equipment.

Texas School for the Deaf (TSD), hereinafter referred to as School, provides for a system of computers and voice and data networks, including the Internet, to promote educational excellence, to promote resource sharing, to promote innovative instruction and communication, and to prepare students to live and work in the 21st century. The Superintendent or designee shall implement, monitor, and evaluate electronic media resources for instructional and administration purposes.

AVAILABILITY OF ACCESS

Access to the School’s technology resources, including the Internet, shall be made available to students, employees, and other authorized users primarily for educational and administrative purposes and in accordance with administrative regulations.

LIMITED PERSONAL USE

Limited personal use of the system shall be permitted if the use:

1. Imposes no tangible cost on the School;
2. Does not unduly burden the School’s technology resources;
3. Has no adverse effect on an employee’s job performance or on a student’s academic performance.

USE BY MEMBERS OF THE PUBLIC

Access to the School’s technology resources, including the Internet, shall be made available to members of the public, in accordance with administrative regulations. Such use shall be permitted so long as the use:

1. Imposes no tangible cost on the School; and
2. Does not unduly burden the School’s technology resources.

NEXT GENERATION

The School, in the administration of the school, shall consider using next generation technologies, including cryptocurrency, blockchain technology, robotic process automation, and artificial intelligence. Gov’t Code 2054.601

CHILDREN’S INTERNET PROTECTION ACT (CIPA)

DEFINITIONS

Harmful to Minors

“Harmful to minor” means any picture, image, graphic image file, or other visual depiction that:

1. Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;
2. Depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and

3. Taken as a whole, lacks serious literary, artistic, political, or scientific value as a to minors.

47 U.S.C. 254(h)(7)(G); 20 U.S.C. 7131(e)(6)

Technology Protection Measure

"Technology protection measure" means a specific technology that blocks or filters internet access to the material covered by a certification described at Certifications to the FCC, below, to which such certification relates. *47 U.S.C. 254(h)(7)(I)*

Universal Service Discounts (E-Rate)

An elementary or secondary school having computers with internet access may not receive universal service discount rates unless the district submits to the FCC the certifications described below at Certifications to the FCC and a certification that an internet safety policy has been adopted and implemented as described at Internet Safety Policy, below, and ensures the use of computers with internet access in accordance with the certifications. *47 U.S.C. 254(h)(5)(A); 47 C.F.R. 54.520*

Certifications to the FCC

A district that receives discounts for internet access and internal connections services under the federal universal service support mechanism for schools must make certifications in accordance with 47 C.F.R. 54.520© each funding year. A district that only receives discounts for telecommunications services is not subject to the certification requirements, but must indicate that it only receives discounts for telecommunications services. *47 C.F.R. 54.520(b)*

With Respect to Minors

A certification under 47 U.S.C. 254(h)(5)(B) is a certification that the School is:

1. Enforcing a policy of internet safety for minors that includes monitoring their online activities and the operation of a technology protection measure with respect to any of its computers with internet access that protects against access through such computers to visual depictions that are obscene, child pornography, or harmful to minors;

2. Enforcing the operation of such technology protection measure during any use of such computers by minors; and

3. Educating minors, as part of its internet safety policy, about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.

47 U.S.C. 254(h)(5)(B); 47 U.S.C. 54.520(c)(1)

With Respect to Adults

A certification under 47 U.S.C. 254(h)(5)© is a certification that the district is:

1. Enforcing a policy of internet safety that includes the operation of a technology protection measure with respect to any of its computers with internet access that protects against access through such computers to visual depictions that are obscene or child pornography; and
2. Enforcing the operation of such technology protection measure during any use of such computers.

47 U.S.C. 254(h)(5)©; 47 C.F.R. 54.520©(1)

Disabling for Adults

An administrator, supervisor, or other person authorized by the School may disable the technology protection measure during use by an adult to enable access for bona fide research or other lawful purpose. *47 U.S.C. 254(h)(5)(D)*

Internet Safety Policy

A district shall adopt and implement an internet safety policy that addresses:

1. Access by minors to inappropriate matter on the internet and the World Wide Web;
2. The safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications;
3. Unauthorized access, including “hacking,” and other unlawful activities by minors online;
4. Unauthorized disclosure, use, and dissemination of personal identification information regarding minors; and
5. Measures designed to restrict minor’s access to materials harmful to minors.

47 U.S.C. 254(l); 47 C.F.R. 54.520(c)(1)(ii)

Public Hearing

The School shall provide reasonable public notice and hold at least one public hearing or meeting to address the proposed internet safety policy. *47 U.S.C. 254(h)(5)(A)(iii), (l)(1)(B)*

Inappropriate for Minors

A determination regarding what matter is inappropriate for minors shall be made by the board or designee. *47 U.S.C. 254(l)(2)*

Noncompliance

A district that knowingly fails to submit required certifications shall not be eligible for discount services under the federal universal service support mechanism for schools until such certifications are submitted.

A district that knowingly fails to ensure the use of computers in accordance with the required certifications must reimburse any funds and discounts received under the federal universal service support mechanism for schools for the period in which there was noncompliance.

47 C.F.R. 54.520(d), (e); 47 U.S.C. 254(h)(5)(F)

ESEA Funding

No federal funds made available under Title IV, Part A of the ESEA for an elementary or secondary school that does not receive universal service discount rates may be used to purchase computers used to access the internet, or to pay for direct costs associated with accessing the internet unless the School:

1. Has in place a policy of internet safety for minors that includes the operation of a technology protection measure that protects against access to visual depictions that are obscene, child pornography, or harmful to minors; and enforces the operation of the technology protection measure during any use by minors of its computers with internet access; and
2. Has in place a policy of internet safety that includes the operation of a technology protection measure that protects against access to visual depictions that are obscene or child pornography; and enforces the operation of the technology protection measure during any use of its computers with internet access.

An administrator, supervisor, or other person authorized by the School may disable the technology protection measure to enable access for bona fide research or other lawful purposes.

Certification to U.S. Department of Education

The School shall certify its compliance with these requirements during each annual program application cycle under the ESEA.

20 U.S.C. 7131

ACCEPTABLE USE	The Superintendent or designee shall develop and implement administrative regulations, guidelines, and user agreements consistent with the purpose and mission of the School and with applicable laws and policies. Access to the School's technology resources is a privilege, not a right. All users shall be required to acknowledge receipt and understanding of all administrative regulations governing use of the School's technology resources and shall agree in writing to allow monitoring of their use and to comply with such regulations and guidelines. Noncompliance may result in suspension of access or termination of privileges regardless of whether any other disciplinary action is taken. Violations of law may result in criminal prosecution as well as disciplinary action by the School.
SOCIAL MEDIA	The use of social media including social networking sites, such as Facebook, X (formerly known as Twitter), Instagram, LinkedIn and others, and video sharing web sites such as YouTube and others, shall adhere to the School's "Social Media Administrative Procedure" available on the TSD website.
STUDENT PARTICIPATION IN SOCIAL MEDIA	Under appropriate system controls and supervision, participation in approved social media using the School's technology resources for educational and administrative purposes is permissible for students and staff. Students participating in social media using the School's technology resources should assume that all content shared, including pictures is public. No personally identifying information should be published. Students should not respond to requests for personally identifying information or contacts from unknown individuals.
FILTERING	The School shall have an Internet filtering device or software that can block access to visual depictions that are obscene, pornographic, inappropriate for students, or harmful to minors, as defined by the federal Children's Internet Protection Act and as determined by the Superintendent or designee. The Superintendent or designee shall enforce the use of such filtering devices. Upon approval from the Superintendent or designee, an administrator, supervisor, or other authorized person may disable the filtering device for bona fide research or other lawful purpose.
MONITORED USE	Electronic mail transmissions and other use of the School's technology resources by students, employees, and members of the public shall not be considered private. Designated School staff shall be authorized to monitor such communication at any time to ensure appropriate use.

PERSONAL TECHNOLOGY RESOURCES	Students, employees and guests may connect personal technology resources to the School's network for educational purposes as set forth by the Superintendent or designee.
SOFTWARE	All software used in the School must be legally licensed and approved. All School-funded software shall be approved and installed by technology department staff or a designee.
DONATED RESOURCES	Donated technology resources may be accepted if the equipment and or software meets or exceeds the minimum standards as set forth by the Superintendent or designee. All donated technology resources shall become the property of the School.
DISCLAIMER OF LIABILITY	The School shall not be liable for users' inappropriate use of the School's technology resources, violations of copyright restrictions or other laws, users' mistakes or negligence, and costs incurred by users. The School shall not be responsible for ensuring the availability of the School's technology resources or the accuracy, age appropriateness, or usability of any information found on the Internet.
UNIFORM ELECTRONIC TRANSACTIONS ACT (UETA)	The UETA (Business and Commerce Code Chapter 322) applies to electronic records and electornic signatures relating to a transaction. Business and Commerce Code 322.003(a). The UETA applies only to transactions between parties each of which has agreed to conduct transactions by electronic means. The UETA does not require a record or signature to be created, generated, sent, communicated, received, stored, or otherwise processed or used by electronic means or in electronic form. A party that agrees to conduct a transaction by electronic means may refuse to conduct other transactions by electronic means. This right may not be waived by agreement. *Business and Commerce Code 322.005(a)–(c)* Except as otherwise provided in Business and Commerce Code 322.012(f), the UETA does not require a district to use or permit the use of electronic records or electronic signatures. *Business and Commerce Code 322.017(c)*
RECORD RETENTION	If a law requires that a record be retained, the requirements is satisfied by retaining an electronic record of the information in the record which: 1. Accurately reflects the information set forth in the record after it was first generated in its final form as an electronic record or otherwise; and 2. Remains accessible for later reference.

A record retained as an electronic record in accordance with the provisions above satisfies a law requiring a person to retain a record of evidentiary, audit, or like purposes, unless a law enacted after January 1, 2002, specifically prohibits the use of an electronic record for the specified purpose.

Business and Commerce Code 322.012(a), (f)

[For more information on records management, see CPC.]

DEFINITIONS

"Electronic record" means a record created, generated, sent, communicated, received, or stored by electronic means.

"Electronic signature" means an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.

"Transaction" means an action or set of actions occurring between two or more persons relating to the conduct of business, commercial, or governmental affairs.

Business and Commerce Code 322.002(7), (8), (15)

DIGITAL SIGNATURE

A digital signature may be used to authenticate a written electronic communication sent to a district if it complies with rules adopted by the board. Before adopting the rules, the board shall consider the rules adopted by the Department of Information Resources (DIR) and, to the extent possible and practicable, make the board's rules consistent with DIR rules. *Gov't Code 2054.060(b)* [See 1 Administrative Code Chapter 203 for DIR rules related to management of electronic transactions and signed records.]

"Digital signature" means an electronic identifier intended by the person using it to have the same force and effect as the use of a manual signature. *Gov't Code 2054.060(e)(1)*

INTERCEPTION OF COMMUNICATIONS

For information on the unlawful interception, use, or disclosure of communications, see the Electronic Communications Privacy Act (18 USC 2510–2523 [federal wiretap act] and 2701–2713 [Stored Communications Act]) and Penal Code 16.02 (state wiretap law) and 16.04 (Unlawful Access to Stored Communications).

SECURITY BREACH NOTIFICATION

Upon discovering or receiving notification of a breach of system security, the School shall disclose the breach to affected persons or entities in accordance with the time frames established by law.

The School shall give notice by using one or more of the following methods:

2. Written notice.
3. Electronic mail, if the School has electronic mail addresses for the affected persons.
4. Conspicuous posting on the School's Web site.
5. Publication through broadcast media.

Adopted:	02-06-87	Reviewed:	02-11-16	Amended:	08-16-91	07-02-10
					10-09-98	08-10-12
					08-28-99	12-14-12
					10-13-00	02-16-17
					08-10-01	08-25-17
					03-05-04	04-30-21
						04-12-24