Next Generation Technology

An ESC, in the administration of the ESC, shall consider using next generation technologies, including cryptocurrency, blockchain technology, and artificial intelligence. *Gov't Code 2054.601*

Children's Internet Protection Act

Definitions

"Harmful to minors" 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 to minors.

47 U.S.C. 254(h)(7)(G); 20 U.S.C. 6777(e)(6)

"Technology protection measure" means a specific technology that blocks or filters internet access to 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 ESC having computers with internet access may not receive universal service discount rates unless the ESC implements an internet safety policy, submits certifications to the FCC, and ensures the use of computers with internet access is in accordance with the certifications. *47 U.S.C. 254(h)(5)(A),(I); 47 C.F.R. 54.520*

An ESC that acts as a billed entity for providing internet access or internal connections to schools that receive universal service discounts must certify to the FCC that the school district is enforcing an internet safety policy. A school receiving such services from an ESC must implement an internet safety policy, submit certifications to the ESC, and ensure the use of computers with internet access is in accordance with the certifications. *47 U.S.C. 254(h)(5)(A),(I); 47 C.F.R. 54.520*

"Universal service" means telecommunications services including internet access, internet services, and internal connection services and other services that are identified by the FCC as eligible for federal universal service support mechanisms. *47 U.S.C. 254(c), (h)(5)(A)(ii)*

Internet Safety Policy

An ESC 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 minors' access to materials harmful to minors.

47 U.S.C. 254(l); 7 C.F.R. 54.520(c)(1)(ii)

As part of its internet safety policy, ESCs must educate minors 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)(iii)*

Public Hearing

An ESC 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), (l)(1)*

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

An ESC 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.

An ESC 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)

Technology Protection Measure

In accordance with the appropriate certification, an ESC shall operate a technology protection measure that protects minors against access to visual depictions that are obscene, child pornography, or harmful to minors; and protects adults against access to visual depictions that are obscene or child pornography. *47 U.S.C. 254(h)(5)(B), (C)*

Exception for Adults

An administrator, supervisor, or other person authorized by an ESC 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)*

Monitored Use

In accordance with the appropriate certification, an ESC shall monitor the online activities of minors. *47 U.S.C. 254(h)(5)(B)*

Certifications to the FCC

To be eligible for universal service discount rates, an ESC shall certify to the FCC during each annual program application cycle, in the manner prescribed at 47 C.F.R. 54.520, that:

1. An internet safety policy has been adopted and implemented;
2. With respect to use by minors, an ESC is enforcing the internet safety policy and operating a technology protection measure during any use of the computers; and
3. With respect to use by adults, an ESC is enforcing an internet safety policy and operating a technology protection measure during any use of the computers.

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

ESEA Funding

No federal funds made available under Title II, Part D 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 an ESC:

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 ESC may disable the technology protection measure to enable access to bona fide research or for another lawful purpose.

Certification to the Department of Education

An ESC shall certify its compliance with these requirements to the

Department of Education as part of the annual application process for each program funding year under the ESEA.

20 U.S.C. 7131

Uniform Electronic Transactions Act

The Uniform Electronic Transactions Act (UETA) (Business and Commerce Code Chapter 322) applies to electronic records and electronic 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 an ESC to use or permit the use of electronic records or electronic signatures. *Business and Commerce Code 322.017(c)*

Records Retention

If a law requires that a record be retained, the requirement 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 for 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)

Authentication of Electronic Communications

A digital signature may be used to authenticate a written electronic communication sent to an ESC if it complies with rules adopted by the board. Before adopting the rules, the board shall consider the rules adopted by the Texas Department of Information Resources (DIR) and, to the extent possible and practicable, shall make the board's rules consistent with DIR rules. *Gov't Code 2054.060(b); 1 TAC 203*

"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 U.S.C. 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).