Children's Internet Protection Act

Under the Children's Internet Protection Act (CIPA), an ESC must, as a prerequisite to receiving universal service discount rates, implement certain Internet safety measures and submit certification to the Federal Communications Commission (FCC). *47 U.S.C. 254* [See UNIVERSAL SERVICE DISCOUNTS, below, for details]

ESCs that do not receive universal service discounts but do receive certain federal funds under the Elementary and Secondary Education Act (ESEA) must, as a prerequisite to receiving these funds, implement certain Internet safety measures and submit certification to the Department of Education (DOE). *20 U.S.C. 6777* [See ESEA FUNDING, below, for details]

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. *47 U.S.C. 254(h)(7)(I)*

Universal Service Discounts

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)

As part of its Internet safety policy, ESCs must educate minors about appropriate online behavior, including interacting with other individuals on social networking Web sites 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)*

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.
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

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 not 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 ESC may disable the technology protection measure to enable access to bona fide research or for another lawful purpose.

Certification to DOE

An ESC shall certify its compliance with these requirements to the DOE as part of the annual application process for each program funding year under the ESEA.

20 U.S.C. 6777

Security Breach Notification

To Individuals

An ESC that owns or licenses computerized data that includes sensitive personal information shall disclose, in accordance with the notice provisions at Business and Commerce Code 521.053(e), any breach of system security, after discovering or receiving notification of the breach, to any individual whose sensitive personal information was, or is reasonably believed to have been, acquired by

	an unauthorized person. The disclosure shall be made as quickly as possible, except as provided at CRIMINAL INVESTIGATION EXCEPTION, below, or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system.
To the Owner or License Holder	An ESC that maintains computerized data that includes sensitive personal information not owned by the ESC shall notify the owner or license holder, in accordance with Business and Commerce Code 521.053(e), of the information of any breach of system security immediately after discovering the breach, if the sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
To a Consumer Reporting Agency	If an ESC is required to notify at one time more than 10,000 persons of a breach of system security, the ESC shall also notify each consumer reporting agency, as defined by 15 U.S.C. 1681a, that maintains files on consumers on a nationwide basis, of the timing, distribution, and content of the notices. The ESC shall provide the notice without unreasonable delay.
Criminal Investigation Exception	An ESC may delay providing the required notice to state residents or the owner or license holder at the request of a law enforcement agency that determines that the notification will impede a criminal investigation. The notification shall be made as soon as the law enforcement agency determines that the notification will not compromise the investigation.
Information Security Policy	An ESC that maintains its own notification procedures as part of an information security policy for the treatment of sensitive personal information that complies with the timing requirements for notice described above complies with Business and Commerce Code 521.053 if the ESC notifies affected persons in accordance with that policy. *Business and Commerce Code 521.053; Gov't Code 205.010*
Definitions	"Breach of system security" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person, including data that is encrypted if the person accessing the data has the key required to decrypt the data. Good faith acquisition of sensitive personal information by an employee or agent of the person for the purposes of the person is not a breach of system security unless the person uses or discloses the sensitive personal information in an unauthorized manner. *Business and Commerce Code 521.053(a)* "Sensitive personal information" means:

1. An individual's first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted:

    a. Social security number;

    b. Driver's license number or government-issued identification number; or

    c. Account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; or

2. Information that identifies an individual and relates to:

    a. The physical or mental health or condition of the individual;

    b. The provision of health care to the individual; or

    c. Payment for the provision of health care to the individual.

"Sensitive personal information" does not include publicly available information that is lawfully made available to the public from the federal government or a state or local government.

Business and Commerce Code 521.002(a)(2), (b)

Access to Electronic Communications

Electronic Communication Privacy Act

Except as otherwise provided in the Electronic Communication Privacy Act (ECPA), 18 U.S.C. 2510–22, a person commits an offense if the person:

1. Intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept any wire, oral, or electronic communication;

2. Intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when:

    a. Such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication;

    b. Such device transmits communications by radio, or interferes with the transmission of such communication;

    c. Such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce;

d. Such use or endeavor to use takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or

e. Such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States;

3. Intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the prohibited interception of a wire, oral, or electronic communication;

4. Intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the prohibited interception of a wire, oral, or electronic communication; or

5. Intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, intercepted by means authorized by 18 U.S.C. 2511(2)(a)(ii), 2511(2)(b)–(c), 2511(2)(e), 2516, and 2518; knowing or having reason to know that the information was obtained through the interception of such a communication in connection with a criminal investigation; having obtained or received the information in connection with a criminal investigation; and with intent to improperly obstruct, impede, or interfere with a duly authorized criminal investigation.

It shall not be unlawful for a person not acting under the color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any state.

18 U.S.C. 2511(1), (2)(d)

Stored Wire and Electronic Communications and Transactional Records Access Act

An ESC must comply with the stored wire and electronic communications and transactional records access act, 18 U.S.C. 2701–12.

A person is prohibited from obtaining, altering, or preventing authorized access to a wire or electronic communication while it is in electronic storage by:

1. Intentionally accessing without authorization a facility through which an electronic communication service is provided; or
2. Intentionally exceeding an authorization to access that facility.

Exceptions

This section does not apply with respect to conduct authorized:

1. By the person or entity providing a wire or electronic communications service;
2. By a user of that service with respect to a communication of or intended for that user; or
3. By sections 18 U.S.C. 2703, 2704, or 2518.

18 U.S.C. 2701(a), (c)

Definitions

"Electronic Communication"

"Electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate or foreign commerce. *18 U.S.C. 2510(12)*

"Electronic Storage"

"Electronic storage" means:

1. Any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and
2. Any storage of such communication by an electronic communication service for purposes of backup protection of such communication.

18 U.S.C. 2510(17)

Messages that have been sent to a person, but not yet opened, are in temporary, intermediate storage and are considered to be in electronic storage. *See Steve Jackson Games, Inc. v. United States Secret Service*, 36 F.3d 457 (5th Cir. 1994). Electronic communications that are opened and stored separately from the provider are considered to be in post-transmission storage, not electronic storage. *See Fraser v. Nationwide Mut. Ins. Co.*, *352 F.3d 107 (3d Cir. 2004).*

"Electronic Communications System"	"Electronic communications system" means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications. *18 U.S.C. 2510(14)*
"Electronic Communications Service"	"Electronic communication service" means any service that provides to users thereof the ability to send or receive wire or electronic communications. *18 U.S.C. 2510(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 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; 1 TAC 203*