

ELECTRONIC COMMUNICATION AND DATA MANAGEMENT

CQ
(LEGAL)

PEIMS	<p>The District shall participate in the Public Education Information Management System (PEIMS) and through that system shall provide information required for the administration of the Foundation School Program and of other appropriate provisions of the Education Code. The PEIMS data standards, established by the Commissioner, shall be used by the District to submit information. <i>Education Code 42.006; 19 TAC 61.1025</i></p>
CHILDREN'S INTERNET PROTECTION ACT	<p>Under the Children's Internet Protection Act (CIPA), the District must, as a prerequisite to receiving universal service discount rates, implement certain Internet safety measures and submit certification to the Federal Communications Commission (FCC). <i>47 U.S.C. 254</i> [See UNIVERSAL SERVICE DISCOUNTS, below, for details]</p> <p>Districts 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). <i>20 U.S.C. 6777</i> [See ESEA FUNDING, below, for details]</p>
DEFINITIONS	<p>"Harmful to minors" means any picture, image, graphic image file, or other visual depiction that:</p> <ol style="list-style-type: none">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; and3. Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors. <p><i>47 U.S.C. 254(h)(7)(G); 20 U.S.C. 6777(e)(6)</i></p> <p>"Technology protection measure" means a specific technology that blocks or filters Internet access. <i>47 U.S.C. 254(h)(7)(I)</i></p>
UNIVERSAL SERVICE DISCOUNTS	<p>An elementary or secondary school having computers with Internet access may not receive universal service discount rates unless the District implements an Internet safety policy, submits certifications to the FCC, and ensures the use of computers with Internet access in accordance with the certifications. <i>47 U.S.C. 254(h)(5)(A); 47 CFR 54.520</i></p> <p>"Universal service" means telecommunications services including Internet access, Internet services, and internal connection services</p>

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

The 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 on-line;
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, the District 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

The District 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, the District 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)*

MONITORED USE

In accordance with the appropriate certification, the District shall monitor the on-line activities of minors. *47 U.S.C. 254(h)(5)(B)*

CERTIFICATIONS TO
THE FCC

To be eligible for universal service discount rates, the District shall certify to the FCC, in the manner prescribed at 47 CFR 54.520, that:

1. An Internet safety policy has been adopted and implemented.

ELECTRONIC COMMUNICATION AND DATA MANAGEMENT

CQ
(LEGAL)

2. With respect to use by minors, the District is enforcing the Internet safety policy, educating minors about appropriate online behavior as part of its Internet safety policy, and operating a technology protection measure during any use of the computers.
3. With respect to use by adults, the District is enforcing an Internet safety policy and operating a technology protection measure during any use of the computers, except that an administrator, supervisor, or other person authorized by the District 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); 47 CFR 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 the District:

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.

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

CERTIFICATION TO
DOE

The District 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

TRANSFER OF
EQUIPMENT TO
STUDENTS

The District may transfer to a student enrolled in the District:

1. Any data processing equipment donated to the District, including equipment donated by a private donor, a state elee-

mosynary institution, or a state agency under Government Code 2175.128;

2. Any equipment purchased by the District; and
3. Any surplus or salvage equipment owned by the District.

Education Code 32.102(a)

Before transferring data processing equipment to a student, the District must:

1. Adopt rules governing transfers, including provisions for technical assistance to the student by the District;
2. Determine that the transfer serves a public purpose and benefits the District; and
3. Remove from the equipment any offensive, confidential, or proprietary information, as determined by the District.

Education Code 32.104

DONATIONS

The District may accept:

1. Donations of data processing equipment for transfer to students; and
2. Gifts, grants, or donations of money or services to purchase, refurbish, or repair data processing equipment.

Education Code 32.102(b)

USE OF PUBLIC FUNDS

The District may spend public funds to:

1. Purchase, refurbish, or repair any data processing equipment transferred to a student; and
2. Store, transport, or transfer data processing equipment under this policy.

Education Code 32.105

ELIGIBILITY

A student is eligible to receive data processing equipment under this policy only if the student does not otherwise have home access to data processing equipment, as determined by the District. The District shall give preference to educationally disadvantaged students. *Education Code 32.103*

RETURN OF EQUIPMENT

Except as provided below, a student who receives data processing equipment from the District under this policy shall return the equipment to the District not later than the earliest of:

1. Five years after the date the student receives the equipment;

ELECTRONIC COMMUNICATION AND DATA MANAGEMENT

CQ
(LEGAL)

2. The date the student graduates;
3. The date the student transfers to another district; or
4. The date the student withdraws from school.

If, at the time the student is required to return the equipment, the District determines that the equipment has no marketable value, the student is not required to return the equipment.

Education Code 32.106

UNIFORM
ELECTRONIC
TRANSACTIONS ACT

The District may agree with other parties to conduct transactions by electronic means. Any such agreement or transaction must be done in accordance with the Uniform Electronic Transactions Act. *Business and Commerce Code Chapter 322*

SECURITY BREACH
NOTIFICATION

A district that owns, licenses, or maintains computerized data that includes sensitive personal information shall comply, in the event of a breach of system security, with the notification requirements of Business and Commerce Code 521.053 to the same extent as a person who conducts business in this state. *Local Gov't Code 205.010*