PEIMS

A 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 of education, shall be used by a district to submit information. *Education Code 42.006; 19 TAC 61.1025*

Children's Internet Protection Act

Under the Children's Internet Protection Act (CIPA), a 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). *47 U.S.C. 254*
[See UNIVERSAL SERVICE DISCOUNTS, below, for details]

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). *20 U.S.C. 7131*
[See ESEA FUNDING, below, for details]

Definitions

"Harmful to Minors"

"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. 7131(e)(6)

"Technology Protection Measure"

"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 elementary or secondary school having computers with Internet access may not receive universal service discount rates unless a 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 support mechanism for schools must make certifications in accordance with 47 C.F.R. 54.520(c) 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 district must submit certification that the district:

1. Is 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. Is enforcing the operation of such technology protection measure during any use of such computers by minors; and

3. Is 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)

With Respect to Adults

A district must submit certification that the district:

1. Is 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. Is enforcing the operation of such technology protection measure during any use of such computers.

47 U.S.C. 254(h)(5)(C)

Disabling for Adults

An administrator, supervisor, or other person authorized by a 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)(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 minors' access to materials harmful to minors.

47 U.S.C. 254(l)

Public Hearing A 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)(iii), (l)(1)(B)*

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

ESEA Funding 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 not be used to purchase computers used to access the Internet, or to pay for direct costs associated with accessing the Internet unless a 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.

A district may disable the technology protection measure to enable access for bona fide research or other lawful purposes.

Certification to DOE A district shall certify its compliance with these requirements during each annual program application cycle under the ESEA.

20 U.S.C. 7131

Transfer of Equipment to Students

A 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 eleemosynary institution, or a state agency under Government Code 2175.905;
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, a 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

A 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)

A district shall not pay a fee or other reimbursement to a state eleemosynary institution or institution or agency of higher education or other state agency for surplus or salvage data processing equipment it transfers to the district. *Government Code 2175.905(c)*

Use of Public Funds

A 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 a district. A 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 a 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;
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

A 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; 1 TAC 203*

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; 1 TAC 203*

Security Breach Notification

To Individuals

A district 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

A district that maintains computerized data that includes sensitive personal information not owned by the district shall notify the owner or license holder of the information, in accordance with Business and Commerce Code 521.053(e), 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 a district is required to notify at one time more than 10,000 persons of a breach of system security, the district 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 district shall provide the notice without unreasonable delay.

Criminal Investigation Exception

A district 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

A district 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 district notifies affected persons in accordance with that policy.

Business and Commerce Code 521.053; Local Gov't Code 205.010

Definitions

"Breach of System Security"

"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"

"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, 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; or

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

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; or

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 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

A district must comply with the Stored Wire and Electronic Communications and Transactional Records Access Act, 18 U.S.C. 2701–12.

Whoever intentionally accesses without authorization a facility through which an electronic communication service is provided or intentionally exceeds an authorization to access that facility and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system commits an offense. *18 U.S.C. 2701(a)*

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(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), 2711(1)*

"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), 2711(1)

The term encompasses only the information that has been stored by an electronic communication service provider. Information that an individual stores to the individual's hard drive or cell phone is not in electronic storage under the statute. *Garcia v. City of Laredo, 702 F.3d 788 (5th Cir. 2012)*

"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), 2711(1)*

"Electronic Communication Service" "Electronic communication service" means any service which provides to users thereof the ability to send or receive wire or electronic communications. *18 U.S.C. 2510(15), 2711(1)*

"Facility" "Facility" includes servers operated by electronic communication service providers for the purpose of storing and maintaining electronic storage. The term does not include technology, such as cell phones and computers, that enables the use of an electronic communication service. *Garcia v. City of Laredo, 702 F.3d 788 (5th Cir. 2012)*

"Person" "Person" means any employee, or agent of the United States or any state or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation. *18 U.S.C. 2510(6), 2711(1)*

Cybersecurity Information Sharing Act

A district may, for a cybersecurity purpose and consistent with the protection of classified information, share with, or receive from, any other non-federal entity or the federal government a cyber threat indicator or defensive measure. A district receiving a cyber threat indicator or defensive measure from another entity shall comply with otherwise lawful restrictions placed on the sharing or use of such cyber threat indicator or defensive measure by the sharing entity. *6 U.S.C. 1503(c)*

Protection and Use of Information

Security

A district monitoring an information system, operating a defensive measure, or providing or receiving a cyber threat indicator or defensive measure under 6 U.S.C. 1503 shall implement and utilize a security control to protect against unauthorized access to or acquisition of such indicator or measure. *6 U.S.C. 1503(d)(1)*

Removal of Personal Information

A district sharing a cyber threat indicator pursuant to these provisions shall, prior to sharing:

1. Review such indicator to assess whether it contains any information not directly related to a cybersecurity threat that the district knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual and remove such information; or

2. Implement and utilize a technical capability configured to remove any information not directly related to a cybersecurity threat that the district knows at the time of sharing to be personal information of a specific individual or information that identifies a specific individual.

6 U.S.C. 1503(d)(2)

Use of Information

A cyber threat indicator or defensive measure shared or received may, for cybersecurity purposes:

1. Be used by a district to monitor or operate a defensive measure that is applied to an information system of the district, or an information system of another non-federal entity or a federal entity upon written consent of that other entity; and

2. Be otherwise used, retained, and further shared by a district subject to an otherwise lawful restriction placed by the sharing entity on such indicator or measure, or an otherwise applicable provision of law.

6 U.S.C. 1503(d)(3)

Exception	A cyber threat indicator or defensive measure shared with a state, tribal, or local government under Title 6, United States Code, may not be used by any such government to regulate, including an enforcement action, the lawful activity of any non-federal entity or any activity taken by a non-federal entity pursuant to mandatory standards, including an activity relating to monitoring, operating a defensive measure, or sharing of a cyber threat indicator. A cyber threat indicator or defensive measure shared as described in this provision may, consistent with a state, tribal, or local government regulatory authority specifically relating to the prevention or mitigation of cybersecurity threats to information systems, inform the development or implementation of a regulation relating to such information systems. *6 U.S.C. 1503(d)(4)(C)*
Law Enforcement Use	A district that receives a cyber threat indicator or defensive measure under Title 6, United States Code, may use such indicator or measure for the purposes described in 6 U.S.C. 1504(d)(5)(A). *6 U.S.C. 1503(d)(4)(B)* [See CKE]
Exemption from Public Disclosure	A cyber threat indicator or defensive measure shared by or with a state, tribal, or local government under 6 U.S.C. 1503 shall be deemed voluntarily shared information and exempt from disclosure under any state or local freedom of information law, open government law, open meetings law, open records law, sunshine law, or similar law requiring disclosure of information or records. *6 U.S.C. 1503(d)(4)(B)* A cyber threat indicator or defensive measure shared with the federal government under Title 6, United States Code, shall be: 1. Deemed voluntarily shared information and exempt from disclosure under federal public information law and any state or local provision of law requiring disclosure of information or records; and 2. Withheld, without discretion, from the public under federal public information law and any state or local provision of law requiring disclosure of information or records. *6 U.S.C. 1504(d)(3)* [See GBA]
No Duty	Nothing in these provisions creates a duty to share a cyber threat indicator or defensive measure or to warn or act based on receipt of a cyber threat indicator or defensive measure; or undermines or limits the availability of otherwise applicable common law or statutory defenses. *6 U.S.C. 1505(c)*
Definitions *"Non-Federal Entity"*	"Non-federal entity" means any private entity, non-federal government agency or department, or state, tribal, or local government

(including a political subdivision, department, or component thereof). *6 U.S.C. 1501(14)*

"Cybersecurity Purpose" "Cybersecurity purpose" means the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability. The term does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement. *6 U.S.C. 1501(4)*

"Cybersecurity Threat" "Cybersecurity threat" means an action, not protected by the First Amendment to the United States Constitution, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that it stored on, processed by, or transiting an information system. *6 U.S.C. 1501(5)*

"Cyber Threat Indicator" "Cyber threat indicator" means information that is necessary to describe or identify:

1. Malicious reconnaissance, as defined in 6 U.S.C. 1501(12), including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability;
2. A method of defeating a security control or exploitation of a security vulnerability;
3. A security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability;
4. A method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability;
5. Malicious cyber command and control, as defined in 6 U.S.C. 1501(11);
6. The actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat;
7. Any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or
8. Any combination thereof.

6 U.S.C. 1501(6)

"Defensive Measure"	"Defensive measure" means an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability. The term does not include a measure that destroys, renders unusable, provides unauthorized access to, or substantially harms an information system or information stored on, processed by, or transiting such information system not owned by the private entity operating the measure or another entity that is authorized to provide consent and has provided consent to that private entity for operation of such measure. *6 U.S.C. 1501(7)*
"Information System"	"Information system" has the meaning given the term in 44 U.S.C. 3502 and includes industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers. *6 U.S.C. 1501(9)*
"Security Control"	"Security control" means the management, operational, and technical controls used to protect against an unauthorized effort to adversely affect the confidentiality, integrity, and availability of an information system or its information. *6 U.S.C. 1501(16)*
"Security Vulnerability"	"Security vulnerability" means any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control. *6 U.S.C. 1501(17)*