



# TSBA LEGAL REFERENCE

Policy:

**Use of the Internet**

Section:

**4**

Page:

**1**

**TCA 10-7-512. Electronic mail communications systems — Monitoring of electronic mail communications — Policy required.** — (a) On or before July 1, 2000, the state or any agency, institution, or political subdivision thereof that operates or maintains an electronic mail communications system shall adopt a written policy on any monitoring of electronic mail communications and the circumstances under which it will be conducted.

(b) The policy shall include a statement that correspondence of the employee in the form of electronic mail may be a public record under the public records law and may be subject to public inspection under this part.

**TCA 39-14-602. Violations.—Penalties.** — (a) Whoever knowingly, directly or indirectly, accesses, causes to be accessed, or attempt to access any telephone system, telecommunications facility, computer software, computer program data, computer, computer system, computer network or any part thereof, for the purpose of:

(1) Obtaining money, property or services for oneself or another by means of false or fraudulent pretenses, representations or promises violates this subsection and is subject to the penalties of § 39-14 -105;

(2) Causing computer output to purposely be false, for, but not limited to, the purpose of obtaining money, property, or services for oneself or another by means of false or fraudulent pretenses, representations or promises violates this subsection and is subject to the penalties of § 39-14-105.

(b) Whoever intentionally and without authorization, directly or indirectly:


(1) Accesses any computer, computer system or computer network commits a Class C misdemeanor;

(2) Alters, damages, destroys or attempts to damage or destroy, or causes the disruption to the proper operation of any computer or who performs an act which is responsible for the disruption of any computer, computer system, computer network, computer software, program or data which resides or exists internal or external to a computer, computer system or computer network is punishable as in § 39-14-105;

(3) Introduces or is responsible for the input of any computer containment into any computer, computer system, or computer network commits a Class B misdemeanor; or

(4) Accesses or causes to be accessed, or attempts to access any computer software, computer program, data, computer, computer system, computer network or any part thereof, for the purpose of gaining access to computer material or to tamper with computer security devices, including, but not limited to, system hackers, commits a Class A misdemeanor.

(c) Whoever receives, conceals, uses or aids another in receiving, concealing or using any proceeds resulting from a violation of either subsection (a) or subdivision (b)(2), knowing the same to be proceeds of such violation, or whoever receives, conceals, uses or aids another in receiving, concealing or using any books, records, documents, property, financial instrument, computer

	<b>TSBA LEGAL REFERENCE</b>		
	Policy:  <b>Use of the Internet</b>	Section:  <b>4</b>	Page:  <b>2</b>

software, program, or other material, property or objects, knowing the same to have been used in violating either subsection (a) or subdivision (b)(2) is subject to the penalties of § 39-14-105.

*Federal-State Joint Board on Universal Service*, CC Docket No. 96-45, Report and Order (March 30, 2001) —(relevant excerpts)

## II. Executive Summary

3. In this Order, we adopt rules that do the following:
  - In order to receive discounts for Internet access and internal connections services under the universal service support mechanism, school and library authorities must certify that they are enforcing a policy of Internet safety that includes measures to block or filter Internet access for both minors and adults to certain visual depictions. These include visual depictions that are (1) obscene, or (2) child pornography, or with respect to use of computers with Internet access by minors, (3) harmful to minors. An authorized person may disable the blocking or filtering measure during any use by an adult to enable access for bona fide research or other lawful purpose.
  - A school administrative authority must certify that its policy of Internet safety includes monitoring the online activities of minors.
  - In order to receive discounts, school and library authorities must also certify that they have adopted and implemented an Internet safety policy addressing (i) access by minors to inappropriate matter on the Internet and World Wide Web; (ii) the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications; (iii) unauthorized access, including so-called "hacking," and other unlawful activities by minors online; (iv) unauthorized disclosure, use and dissemination of personal information regarding minors; and (v) measures designed to restrict minors access to materials harmful to minors.

## J . Public Notice and Hearing Requirements

49. Section 254(h)(5)(A)(iii) of CIPA establishes that a school, school board, local educational agency, or other authority with responsibility for administration of the school, shall provide reasonable public notice and hold at least one public hearing or meeting to address a proposed Internet safety policy. Under the parallel provision for libraries, CIPA requires that a library shall provide such notice and such a hearing. Furthermore, section 254(l) requires that school and libraries adopting the requisite Internet safety policy under that section also provide reasonable public notice and at least one public meeting or hearing to address that proposed policy.

	<b>TSBA LEGAL REFERENCE</b>		
	Policy:  <b>Use of the Internet</b>	Section:  <b>4</b>	Page:  <b>3</b>

**(c) Certifications required under 47 U.S.C. § 254(h) and (l).**

(1) Schools. The billed entity for a school receives discounts for Internet access or internal connections must certify on FCC Form 486 that an Internet safety policy is being enforced. If the school is an eligible member of a consortium but is not the billed entity for the consortium, the school must certify instead on FCC Form 479 ("Certification to Consortium Leader of Compliance with the Children's Internet Protection Act") that an Internet safety policy is being enforced.

(i) The Internet safety policy adopted and enforced pursuant to 47 U.S.C. § 254(h) must include:

(A) A technology protection measure that protects against Internet access by both adults and minors to visual depictions that are obscene, child pornography, or, with respect to use of the computers by minors, harmful to minors. This Internet safety policy must also include monitoring the online activities of minors.

(ii) The Internet safety policy adopted and enforced pursuant to 47 U.S.C. § 254(l) must address all of the following issues:

(A) access by minors to inappropriate matter on the Internet and World Wide Web;

(B) the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications;

(C) unauthorized access, including so-called "hacking," and other unlawful activities by minors online;

(D) unauthorized disclosure, use, and dissemination of personal information regarding minors; and

(E) measures designed to restrict minors' access to materials harmful to minors.

(iii) A school must satisfy its obligations to make certifications by making one of the following certifications required by subsection (c)(1) on FCC Form 486:



# TSBA LEGAL REFERENCE

Policy:

**Use of the Internet**

Section:

**4**

Page:

**4**

(A) The recipient(s) of service represented in the Funding Request Number(s) on this Form 486 has (have) complied with the requirements of the Children's Internet Protection Act, as codified at 47 U.S.C. § 254(h) and (l).

(B) Pursuant to the Children's Internet Protection Act, as codified at 47 U.S.C. § 254(h) and (l), does not apply because of the recipient(s) of service represented in the Funding Request Number(s) on this Form 486 is (are) undertaking such actions, including any necessary procurement procedures, to comply with the requirements of CIPA for the next funding year, but has (have) not completed all requirements of CIPA for this funding year.

(C) The Children's Internet Protection Act, as codified at 47 U.S.C. § 254(h) and (l), does not apply because of the recipient(s) of service represented in the Funding Request Number(s) on this Form 486 is (are) receiving discount services only for telecommunications services.