PHILOSOPHY AND PURPOSE

The District provides network and Internet access to electronic mail, databases, libraries, museums, and other information sources for the following limited purposes:

1. Promote educational excellence in its schools by facilitating resource sharing, innovation, and communication.
2. Improve learning and reach the District's instructional goals.
3. Achieve effective and efficient administration at the District and campus levels.
4. Comply with the Texas Education Agency's guidelines for technology in schools.

Any use of the District's electronic information systems and resources by authorized users must be in furtherance of these limited purposes and conform to the District's expectations for legal, efficient, and ethical use.

INTERNET SAFETY AND LIMITATIONS ON SITE ACCESS

Recognizing that the Internet can give access to sites containing information that is obscene, child pornography, or harmful to minors or that would be otherwise inappropriate for distribution to students, unsuitable for use in the approved curriculum, or irrelevant to accomplishing the District's stated purposes for operating an Internet-accessible network, the District has installed technology protection measures to filter, screen, analyze, and block site content in an effort to make it more difficult for students or staff to gain access to such material through the District's network.

The technology director or designated campus administrators may disable technology protection measures during use by an adult to allow access to otherwise prohibited or blocked sites or information for bona fide research or other acceptable purposes under this policy.

Nonetheless, the District makes no representation that it can control access to all Internet sites. Network users are responsible for their actions in accessing available resources and will be held accountable for receiving information that is inconsistent with the requirements for acceptable and unacceptable use of the network and Internet.

AUTHORIZED USERS

The District permits individuals in the following categories to become authorized users of its computer network and/or have access to the Internet, subject to administrative regulations developed by the technology director and approved by the Superintendent.

1. Campus administrators and campus administrative support employees.

2. Central office administrators (department or division directors) and their administrative support employees.

3. Instructional personnel.

4. Instructional support and student services personnel, i.e., librarians, counselors, and school nurses.

5. Students in grades 7-12. Students in grades K-6 may have access through class accounts and regulations for those accounts.

To become an authorized user, a person must complete an application, sign the User Agreement, and return both forms to the technology director or designee. Minor students applying for a user account must also return a signed Parent Agreement.

GENERAL REQUIREMENTS FOR NETWORK AND INTERNET USE

Student and employee use of the District's computer network and/or access to the Internet must be in accordance with this policy. No account sharing will be permitted, and each authorized user is responsible for all activities, transmissions, or actions that occur under that account identifier.

Any user who identifies a security problem with the network must immediately notify the District technology director and may not communicate the problem to any other person.

MONITORING USE

Use of a personal network account through the District's system is voluntary and constitutes a privilege provided by the District, not a right. All network usage is subject to monitoring, examination, and investigation by the system administrators without prior notice or the specific consent of the user. By signing the User Agreement, each authorized user acknowledges the possibility of such monitoring and consents to it.

Professional employees overseeing student instructional use of the District's computer network or access to the Internet will be vigilant in determining that students are using the District's system only in compliance with this policy to enhance student safety and security, particularly when students are using electronic mail, chat rooms authorized under this policy, and other forms of direct electronic communication.

SUSPENDING OR REVOKING PRIVILEGES

Access to the network, the Internet, or both may be suspended or revoked and user IDs deleted if a student or employee is determined to have violated this policy or the User Agreement each user signs as a condition for obtaining access to the District's network and/or the Internet.

Any user identified as a security risk or who has a history of violations with other computer systems will be denied access to the network. A user whose access has been suspended or revoked may request a conference with the principal and technology director to discuss the basis for that action and have an opportunity to respond. A decision by the technology director to suspend or revoke system privileges may be appealed to the Superintendent or the Board. System privileges are revoked during any appeal.

ACCEPTABLE USE

Any use described below is deemed "acceptable" and consistent with the User Agreement and this policy. The final decision regarding whether any given use of the network or Internet is acceptable lies with the Superintendent or designee, in consultation with the technology director.

1. Supports instructional purposes and goals.
2. Furthers the District's educational and administrative purposes, goals, and objectives.
3. Furthers research related to education and instruction.
4. Does not violate the student code of conduct or employee standards of conduct.
5. Is consistent with network rules established by the technology director.

UNACCEPTABLE USE

Any of the following uses is deemed "unacceptable" and a violation of the User Agreement and this policy. The final decision regarding whether any given use of the network or Internet is unacceptable lies with the Superintendent or designee, in consultation with the technology director.

1. Unauthorized use of copyrighted material, including violating District software licensing agreements. [See EFE]
2. Posting or distribution of threatening, racist, harassing, excessively violent, or obscene material.
3. Personal, political use to advocate for or against a candidate, office-holder, political party, or political position. Research or electronic communications regarding political issues or candidates shall not be a violation when the activity is to fulfill an assignment for class credit.
4. Participating in chat rooms other than those sponsored and overseen by the District.

5. Tampering, i.e., accessing, reading, deleting, copying, or modifying, with the electronic mail of other users, regardless of where the message is displayed or stored.
6. "Hacking," i.e., attempting unauthorized access to any computer whether within the District's network or outside it.
7. Any use that would be unlawful under state or federal law.
8. Unauthorized disclosure, use, or distribution of personal identification information regarding students or employees.
9. Forgery of electronic mail messages or transmission of unsolicited junk e-mail chain messages.
10. Use that violates the Student Code of Conduct or employee standards of conduct.
11. Use related to commercial activities or for commercial gain by a student or employee.
12. Advertisement for purchase or sale of a product.

SERIOUS VIOLATIONS

If the principal determines that a student's or employee's use of the system violates the Student Code of Conduct or employee standards of conduct and that disciplinary action other than or in addition to suspension or revocation of system privileges is warranted, those disciplinary actions will be in accordance with the applicable policies.

SYSTEM OR OTHER USER INTERFERENCE

Users must not attempt to exceed, evade, or change established resource quotas, i.e., allocations of local hard drive storage space or network time. The District quotas are designed to ensure all users have a fair opportunity to access resources.

Vandalism and mischief are prohibited. Vandalism includes any attempt to harm or destroy another user's data on the network or on any network connected to the District's network and any deliberate creation of propagation of a computer virus(es). Mischief includes any interference with another user's work, such as attempts to delete, examine, copy, or modify data, files, fields, or any other element of another user's information.

DISCLAIMER

The District makes no warranties of any kind, expressed or implied, for its network facilities and bears no liability for users' copyright violations; users' inappropriate or tortious use of the network system or resources; any damages incurred by users, including loss of data resulting from the action or inaction of any District employee or a user's errors or omissions; and phone charges, credit card charges, or any other charges incurred by users without prior District authorization and according to established purchasing proce-

dures. The District specifically denies any responsibility for the accuracy, age-appropriateness, or quality of information obtained through its network facilities.

INTELLECTUAL PROPERTY RIGHTS

Students retain the copyright and all other intellectual property rights to works of any kind they create using the District's electronic information resources and system, including those created in fulfillment of course requirements or through participation in extracurricular activities.

The District is the copyright owner of any work created or developed by an employee within the scope of his or her employment, regardless of whether the work is prepared at school using school equipment or out of school using personally owned or other equipment.

PEIMS

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 of Education, shall be used by the 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), 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). *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. 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)*

UNIVERSAL SERVICE DISCOUNTS

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. *47 U.S.C. 254(h)(5)(A); 47 CFR 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)(3), (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)

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.
2. With respect to use by minors, the District 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, 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 Department of Education as part of the annual application process for each program funding year under the ESEA.

20 U.S.C. 6777

STATE FUNDING

A public school that provides a computer used to access the Internet is not eligible for a loan or grant under Subchapter C, Chapter 57, Utilities Code (Telecommunications Infrastructure Fund), unless the school adopts and implements an Internet safety policy under Chapter 32, Subchapter E, of the Education Code or under the federal Children's Internet Protection Act (CIPA). *Education Code 32.202*

"Internet safety policy" in Chapter 32, Subchapter E, of the Education Code means a policy that addresses:

1. Measures designed to restrict access by minors to obscene material on the Internet;
2. The safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications;
3. Unauthorized access and other unlawful activities by minors online; and
4. Unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

"Obscene" has the meaning assigned by Section 43.21 of the Penal Code.

Education Code 32.201

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 eleemosynary 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;
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 43*