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, 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)(I)*

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), (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.
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;

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

TO STATE RESIDENTS

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 resident of this state 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, 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 the 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

The 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" 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)

The Superintendent or designee shall implement, monitor, and evaluate electronic media resources for instructional and administrative purposes.

AVAILABILITY OF ACCESS

LIMITED PERSONAL USE

Access to the District's electronic communications system, including the Internet, shall be made available to students and employees primarily for instructional and administrative purposes and in accordance with administrative regulations. Limited personal use of the system shall be permitted if the use:

1. Imposes no tangible cost to the District;
2. Does not unduly burden the District's computer or network resources; and
3. Has no adverse effect on an employee's job performance or on a student's academic performance.

USE BY MEMBERS OF THE PUBLIC

Access to the District's electronic communications system, including the Internet, shall be made available to members of the public, in accordance with administrative regulations. Such use may be permitted so long as the use:

1. Imposes no measurable cost on the District;
2. Does not unduly burden the District's computer or network resources; and
3. Is for participation in the District's educational related activities.

Members of the public who are granted access shall be required to:

1. Comply with all District rules, regulations, and policies governing appropriate use of the system;
2. Attend training on the District's acceptable use policies; and
3. Submit a signed copy of the Exhibit D form prior to accessing the District's electronic communications system. [See CQ(EXHIBIT)]

ACCEPTABLE USE

The Superintendent or designee shall develop and implement administrative regulations, guidelines, and user agreements, consistent with the purposes and mission of the District and with laws and policies.

Access to the District's electronic communications system is a privilege, not a right. All users shall be required to acknowledge receipt and understanding of all administrative regulations governing use of the system and shall agree in writing to allow monitoring of their use and to comply with such regulations and guidelines. [See CQ Regulations]

NONCOMPLIANCE

Noncompliance with applicable regulations may result in:

1. Verbal or written warning by network administrator or designee;
2. Temporary reduction or suspension of computer system privileges;
3. Referral to immediate supervisor;
4. Permanent access revocation;
5. Termination of employment; or
6. Referral to appropriate law enforcement agencies for misuse amounting to criminal behavior.

Alleged violations shall be reviewed on a case by case basis. Violations of law may result in criminal prosecution as well as disciplinary action by the District. Disciplinary action shall be consistent with District policies. [See DH, FN series, FO series, and the Student Code of Conduct]

IMPROPER PERSONAL INTERNET USE

Student's home and personal Internet use can have an impact on the school and other students. If students' personal Internet expression—such as a threatening message to another student, a District employee, or a violent Web site—creates a likelihood of material disruption of the school's operations, students may face school discipline and criminal penalties.

CYBER HARASSMENT

The District takes bullying, stalking, and harassment by computer very seriously. Students shall not use any Internet or other communication device to intimidate, bully, harass, stalk, or embarrass other students or staff members. Students who engage in such activity on school grounds or who engage in such activity off campus and create a material disruption of school operations shall be subject to penalties for bullying and harassment contained in the student handbook, as well as possible criminal penalties.

MONITORED USE

Internet use, file transfers (FTP), electronic mail transmissions and other uses of the District's electronic communications system by students, employees, and the public, are not private and may be monitored at any time by designated District staff to ensure appropriate use.

STANDARDS FOR PERSONAL EXPRESSION ON THE INTERNET

The following restrictions against inappropriate speech and messages apply to all speech communicated and accessed through the District's Internet system, including all e-mail, instant messages, Web pages, and Web logs. Students and employees shall not send obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful messages. Students and employees shall not post information that could cause damage, danger, or disruption, or engage in personal attacks, including prejudicial or discriminatory attacks. Students shall not harass another person, or knowingly or recklessly post false or defamatory information about a person or organization.

INTERNET SAFETY AND FILTERING

The Superintendent or designee shall develop and implement an Internet safety plan to:

1. Control students' access to inappropriate materials, as well as to materials that are harmful to minors;
2. Ensure student safety and security when using electronic communications;
3. Prevent unauthorized access, including hacking and other unlawful activities;
4. Restrict unauthorized disclosure, use, and dissemination of personally identifiable information regarding students; and
5. Educate students about cyberbullying awareness and response and about appropriate online behavior, including interacting with other individuals on social networking Web sites and in chat rooms.

Each District computer with Internet access shall have a filtering device or software that blocks access to visual depictions that are obscene, pornographic, inappropriate for students, or harmful to minors, as defined by the federal Children's Internet Protection Act and as determined by the Superintendent or designee.

FILTER DISABLING

Students and staff may not disable the District's filtering software at any time when students are using the Internet system if such disabling will cease to protect against access to inappropriate materials. Authorized staff may temporarily or permanently unblock access to sites containing appropriate material if the filtering software has inappropriately blocked access to such sites.

INTELLECTUAL PROPERTY RIGHTS

Students shall retain all rights to work they create using the District's electronic communications system.

As agents of the District, employees shall have limited rights to work they create using the District's electronic communications system. The District shall retain the right to use any product created for its use by an employee even when the author is no longer an employee of the District.

STUDENT DUE PROCESS

In the event of a claim that a student has violated this policy, the District shall provide the student with notice and an opportunity to be heard in the manner set forth in the student handbook.

DISCLAIMER OF LIABILITY

The District shall not be liable for users' inappropriate use of electronic communication resources, violations of copyright restrictions or other laws, users' mistakes or negligence, and costs incurred by users. The District shall not be responsible for ensuring the accuracy, age appropriateness, or usability of any information found on the Internet.

SECURITY BREACH NOTIFICATION

Upon discovering or receiving notification of a breach of system security, the District shall disclose the breach to affected persons or entities in accordance with the time frames established by law.

The District shall give notice by using one or more of the following methods:

1. Written notice.
2. Electronic mail, if the District has electronic mail addresses for the affected persons.
3. Conspicuous posting on the District's Web site.
4. Publication through broadcast media.

The Superintendent or designee shall oversee the District's electronic communications system.

The District's system will be used mainly for administrative and educational purposes consistent with the District's mission and goals. Use of the District's system for personal gain, commercial applications, or political purposes is strictly prohibited.

TRAINING

The District will provide training to employees, students, and members of the public in proper use of the system and will provide users with copies of acceptable use guidelines. All training in the use of the District's system will emphasize ethical use of this resource. Access to the District's system will be granted to users after the appropriate training. Only employees may be exempt from attending certain training workshops by successfully completing the District's workshop related exams (testing out).

COPYRIGHT CONSENT REQUIREMENTS

All users should be aware that any information, software, or graphics on the Internet may be protected by federal copyright laws, regardless of whether a copyright notice appears on the work. Licensing agreements may control redistribution of information from Internet-related systems or from the Internet. Duplication or transmission of such material or downloading shareware may not be undertaken without express authorization.

Copyrighted software or copyrighted data may not be placed on any computer or system connected to the District's network without first obtaining a license or permission from the holder of the copyright, and secondly, obtaining permission from the District's technology department.

SYSTEM ACCESS

Access to the District's electronic communications system shall be governed by the following.

District employees shall be granted access to the District's system after meeting all of the following criteria:

1. Attend, or test out of, the training sessions on computer basics and the appropriate use of the District's electronic communication systems.
2. Submit the employee user agreement form [Exhibit C] with the employee signature and that of the immediate supervisor.
3. Receive a final approval confirmation from the District's technology department.

Students shall be granted access to the District's system after meeting all of following criteria:

1. Attend training session on the appropriate use of the District's electronic communications system.
2. Submit a student user agreement form [Exhibit A or B] with student and parent/guardian signatures. Parent/guardian signature is not required if the student is self dependent. A new Exhibit A or B, whichever is more appropriate, shall be submitted each year.
3. Receive approval from the home campus principal or designee.

Members of the public shall be granted access to the District's system after meeting all of the following criteria:

1. Attend a training session on the appropriate use of the District's electronic communication system.
2. Submit the public (nonschool) user agreement form [Exhibit D] with the person's signature.
3. Receive a final approval confirmation from the District's technology department.

RESTRICTIONS AND PROHIBITIONS ON USE AND ACCESS

Communications and Internet access should be conducted in a responsible and professional manner reflecting the District's commitment to honest, ethical, and nondiscriminatory business practice. In furtherance of these goals the following restrictions and prohibitions apply:

DATA SECURITY

1. Users must safeguard their logon ID and password from disclosure to any person except the staff of the District's technology department. Users shall not access a computer account that belongs to another employee or department (except for an authorized member of the District's technology department). Users shall use their own logon ID and password only, are responsible for all activity on their logon ID, and must report any known or suspected compromise of their ID to their immediate supervisor and the District's technology department.
2. Users given access to student data through the Public Education Information Management System (PEIMS) must sign and abide by the terms of the District's Internet Texas Computer Cooperative Software (ITCCS) access confidentiality agreement form. [See CQ(EXHIBIT)]
3. Unauthorized attempts to circumvent data security; to identify or exploit security vulnerabilities; or to decrypt secure data are prohibited.

4. Attempting to monitor, read, copy, change, delete, or tamper with another employee's electronic communications, files, or software without the express authorization of the user (except for authorized District technology personnel) is prohibited.
5. Knowingly or recklessly running or installing (or causing another to run or install) a program (such as a "worm" or "virus") intended to damage or place an excessive load on a computer system or network is prohibited.
6. Forging the source of electronic communications, altering system data used to identify the source of messages or otherwise obscuring the origination of communications is prohibited.
7. Disclosure of logon ID's, passwords, confidential information, or any file contents (data, video, or audio) on any District computer or network system by network supervisors, administrators, or computer specialists to any unauthorized person is strictly prohibited.

USE OF EQUIPMENT

8. Any use that violates federal, state, or local law or regulation is expressly prohibited.
9. Knowing or reckless interfering with the normal operation of computers, peripherals, or networks is prohibited.
10. Setting up or opening computers, connecting peripherals, or tampering with network equipment without proper authorization is prohibited. This includes, but is not limited to, the removal or addition of hardware such as memory, hard drives, CPUs, CD-ROMs, or the connection or disconnection of network cables and equipment.
11. Connecting unauthorized equipment to the network for any purpose inconsistent with the purposes of the District is prohibited. This includes wired and wireless access.
12. Deliberately wasting computer resources, including bandwidth, disk space, printer paper, or running or installing games or other unauthorized software on District's computers is prohibited. This includes downloading, uploading, streaming and/or burning music and video files.
13. Using the District's network to gain unauthorized access to any computer system is prohibited.

Engaging in prohibited activities will result in the cancellation of system use privileges and the user may be subject to other disciplinary actions consistent with District policies and/or local, state or federal laws. Furthermore, the District may require restitution for costs associated with system restoration. [See DH, FN series, FO series, and the Student Code of Conduct]

TECHNOLOGY SUPERVISORS' RESPONSIBILITIES

The technology supervisors or their designees will:

1. Be responsible for disseminating and enforcing applicable District policies and acceptable use guidelines for the District's system.
2. Ensure that all users of the District's system complete and sign an agreement to abide by District policies and administrative regulations regarding such use. All such agreements will be maintained on file in the principal, or designee's office. Employee and members of the public agreement forms will be maintained on file by the District's technology department.
3. Ensure that employees supervising students who use the District's system provide training emphasizing the appropriate use of this resource.
4. Ensure that all software loaded on computers in the District is consistent with District standards and is properly licensed.
5. Be authorized to monitor or examine all system activities, including electronic mail transmissions, as deemed appropriate to ensure proper use of the system. This includes monitoring of individual computers in classrooms and offices.
6. Be authorized to establish a retention schedule for messages on any electronic bulletin board and to remove messages posted locally that are deemed to be inappropriate.
7. Be authorized to set limits for data storage within the District's system, as needed.
8. Be authorized to disable a filtering device on the system for bona fide research or another lawful purpose.
9. Be authorized to remove, or request to have removed, unauthorized or unofficial Web sites representing the District or a campus on an outside server.

TEACHER RESPONSIBILITIES

Staff must supervise student use of the District Internet system, in a manner that is appropriate to the students' age and the circumstances of use.

INDIVIDUAL USER RESPONSIBILITIES

The following standards will apply to all users of the District's electronic information/communications systems:

ONLINE CONDUCT

1. The use of District's Internet-related system to access, transmit, store, display, or request obscene, pornographic, erotic,

profane, racist, sexist, or other offensive material (including messages, images, video, or sound) that violates the District's harassment policy or creates an intimidating or hostile work environment is prohibited.

2. A student knowingly bringing prohibited materials into the school's electronic environment will be subject to suspension of access and/or revocation of privileges on the District's system and will be subject to disciplinary action in accordance with the Student Code of Conduct.

3. An employee knowingly bringing prohibited material into the school's electronic environment will be subject to disciplinary action in accordance with District policies. [See DH]

4. A member of the public knowingly bringing prohibited material into the school's electronic environment will be subject to disciplinary action as determined by the Superintendent or designee.

5. The individual in whose name a system account is issued will be responsible at all times for its proper use.

6. Teachers are responsible for monitoring all computer use in their rooms, librarians for all computer use in their library, lab instructors are responsible for all computer use in their labs, campus administrators for monitoring computer use campus wide, and department heads for monitoring their office staff.

7. Students may not distribute personal information about themselves or others by means of the electronic communication system.

INFORMATION CONTENT / THIRD-PARTY SUPPLIED INFORMATION

System users and parents of students with access to the District's system should be aware that use of the system may provide access to other electronic communications systems in the global electronic network (Internet) that may contain inaccurate and/or objectionable material. A student who accidentally gains access to such material is expected to discontinue the access as quickly as possible and to report the incident to the supervising teacher. Likewise, employees and members of the public who accidentally gain access to inappropriate sites are expected to exit the site as quickly as possible.

E-MAIL

Electronic mail transmissions on District equipment are not private and may be monitored at any time by designated District staff to ensure appropriate use.

The use of e-mail by employees and students is primarily for educational or work-related use. The transmission of hoaxes and chain letters is strictly prohibited. Both of these types of e-mails burden the District's network, and in some cases are illegal.

Employees are responsible for maintaining their District e-mail account by saving and purging old e-mails. The District will set the limitations on the amount of space allotted per employee on the e-mail server, and length of time e-mail will be retained on the District's server.

Students may access their own personal e-mail accounts at school strictly for educational purposes.

System users should be mindful that use of school-related electronic mail addresses might cause some recipients or other readers of that mail to assume they represent the District or school, whether or not that was the user's intention.

CHAT ROOMS AND NEWSGROUPS

Participation in chat rooms and newsgroups accessed on the Internet is permissible only for students participating in curriculum related projects, under appropriate supervision, and for employees participating in curriculum related projects and for administrative use.

VIDEO CONFERENCING AND VIRTUAL FIELD TRIPS

The connection of video conferencing equipment to the District's network for the purpose of transmitting two-way video/audio signals is permissible for educational and administrative purposes. However, prior to scheduling the event, the technology department should be consulted to determine if connectivity is feasible with the equipment available at the location.

Users who plan to make use of video conferencing or virtual field trips should be aware that certain other video taping guidelines and access costs may be involved.

DISTANCE LEARNING

Employees and students are permitted to use the District's system to participate in distance learning. This includes, but is not limited to, classes for professional development, concurrent enrollment, and virtual schools.

Participants should be aware that the District keeps certain Internet ports closed for security reasons. This, in some cases, may block connections to certain sites used in distance learning environments. The District's network administrators will determine which ports may be opened, and which will remain closed.

VOICE OVER INTERNET PROTOCOL (VOIP)

The monitoring and use of the District's Voice over Internet Protocol (VoIP) network shall be governed by the current local, state, and federal regulations and laws, and the District's applicable policies regarding telephone use.

DEVELOPMENT OF WEB PAGES

Development and posting of Web pages on the District's electronic system is permissible under the following guidelines:

1. The developers of department or campus Web pages must attend the training provided by the District's technology department and adhere to the District's Web creation guidelines.
2. Web pages on the District's electronic system are solely for the purpose of sharing educational information with the community.
3. The technology supervisors or designee may remove any campus or department's Web pages if they are deemed inappropriate.
4. Each campus will designate one trained and qualified person who will maintain and upload the campus Web pages. The principal must approve the Web pages before they are posted.
5. Each department at the District level will designate one trained and qualified person to maintain and upload their department's Web pages. The department's head must approve the Web pages before they are posted.
6. All department and campus Web sites must include a hypertext link back to the District's homepage.
7. Department and campus Web pages must be kept current.
8. Web page development will be allowed by students only as part of an instructional program or promotion of campus activities and under the teacher's direct supervision
9. No original work created by any District student or employee will be posted on a Web page under the District's control unless the District has received written consent from the student (and the student's parent) or employee who created the work. [See CQ(EXHIBIT)]
10. No personally identifiable information about a District student will be posted on a Web page under the District's control unless the District has received written consent from the student's parent or legal guardian. The campus principal or designee will be responsible for obtaining a signed release form prior to uploading the Web page. An exception may be made for "directory information" as allowed by the Family Education Records Privacy Act (FERPA) and District policy. [See CQ(EXHIBIT) and FL]

The following specific guidelines will be used for posting student information without written permission from the student's parent:

Student pictures will not be allowed where the student is identifiable. Exceptions to this are group pictures where the student's face is not identifiable. Wide-angle photographs taken during athletic events would be an example of this case.

TERMINATION / REVOCATION OF SYSTEM USER ACCOUNT

The District may suspend or revoke a system user's access to the District's system upon violation of District policy and/or administrative regulations regarding acceptable use.

Termination of an employee's or a student's access for violation of District policies or regulations will be effective on the date the immediate supervisor or principal receives notice of revocation, or on a future date if so specified in the notice. A campus designee will be responsible for notifying campus staff.

DISCLAIMER

The District's system is provided on an "as is, as available basis." The District does not make any warranties, whether express or implied, including, without limitation, those of merchantability and fitness for a particular purpose with respect to any services provided by the system and any information or software contained therein. The District does not warrant that the functions or services performed by, or that the information or software contained on the system will meet the system user's requirements, or that the system will be uninterrupted or error free, or that defects will be corrected.

Opinions, advice, services, and all other information expressed by system users, information providers, service providers, or other third-party individuals in the system are those of the providers and not the District.

The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the District's electronic communications system.

AMENDMENTS

The District may amend the policy or regulation regarding electronic communications from time to time as necessary. All users will receive prompt notice of any amendments.