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

The District will provide training in proper use of the system and will provide all users with copies of acceptable use guidelines. All training in the use of the District's system will emphasize the ethical and safe use of this resource.

Consent Requirements

Copyrighted software or data may not be placed on any system connected to the District's system without permission from the holder of the copyright. Only the copyright owner or individual the owner specifically authorizes may upload copyrighted material to the system.

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, if the student is a minor) or employee who created the work. [See CQ(EXHIBIT)]

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. An exception may be made for "directory information" as allowed by the Family Educational Rights and Privacy Act (FERPA) and District policy. [See CQ(EXHIBIT) and policies at FL]

Filtering

The Superintendent will appoint a committee, to be chaired by the technology director, to select, implement, and maintain appropriate technology for filtering Internet sites containing material considered inappropriate or harmful to minors. All Internet access will be filtered for minors and adults on computers with Internet access provided by the school. The categories of material considered inappropriate and to which access will be blocked will include, but not be limited to, nudity/pornography; images or descriptions of sexual acts; promotion of violence, illegal use of weapons, drug use, discrimination, or participation in hate groups; instructions for performing criminal acts (e.g., bomb making); and online gambling.

Requests to Disable Filter

The Superintendent or designee will consider requests from users who wish to use a blocked site for bona fide research or other lawful purposes.

System Access

Access to the District's electronic communications system will be governed as follows:

1. Students will have access to the District's resources for class assignments and research with their teacher's permission and/or supervision.

2. With the approval of the immediate supervisor and completion of required District network training, District employees will be granted access to the District's system. A teacher may apply for a class or project e-mail account and in doing so will be ultimately responsible for use of the account.
3. Campus employees will be granted access to the District's system for the purpose of sending communications on behalf of teacher professional organizations providing support to campus employees. Campus employees are prohibited from using such access to communicate with any employee who indicates that he or she does not wish to receive such communications. Campus employees sending communications under this provision must comply with all provisions of the District's Acceptable Use Policy and Guidelines.
4. All District employees and students with accounts will be required to maintain password confidentiality by not sharing their password with others.
5. Any system user identified as a security risk or having violated the District's Acceptable Use Guidelines may be denied access to the District's system. Other consequences may also result as well.
6. All users are required to review the Acceptable Use Guidelines annually for issuance or renewal of an account.

Technology Director Responsibilities

The technology director 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 annually review the District's policies and administrative regulations (Acceptable Use Guidelines) regarding such use.
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 student safety online and proper use of the system.
6. Be authorized to disable a filtering device on the system for bona fide research or another lawful purpose, with approval from the Superintendent.

7. Be authorized to remove messages posted locally that are deemed inappropriate.

8. Set limits for data storage within the District's system, as needed.

Campus-Level Coordinator Responsibilities

As the campus-level coordinator for the network systems, the principal or designee will:

1. Be responsible for disseminating and enforcing the District Acceptable Use Guidelines for the District's system at the campus level.

2. Ensure that employees supervising students who use the District's systems provide information emphasizing the appropriate and ethical use of this resource.

Acceptable Use

The District's technology resources will be used only for learning, teaching, and administrative purposes consistent with the District's mission and goals. Commercial use of the District's system is strictly prohibited.

The District will make training available to all users in the proper use of the system and will make copies of Acceptable Use Guidelines available to all users. All training in the use of the District's system will emphasize the ethical use of this resource.

Software or external data may not be placed on any computer, whether stand-alone or networked to the District's system, without permission from the Superintendent or designee.

Individual User Responsibilities

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

Online Conduct

All Users

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

2. The system may not be used for illegal purposes, in support of illegal activities, or for any other activity prohibited by District policy or guidelines.

3. Student use of the computers and computer network is only allowed when supervised or when permission is granted by a staff member.

4. Attempting to log on or logging on to a computer or e-mail system by using another's password is prohibited; assisting others in violating this rule by sharing information or passwords is unacceptable.

5. Improper use of any computer or the network is prohibited. This includes the following:

a. Submitting, publishing, or displaying any defamatory, inaccurate, racially offensive, abusive, obscene, profane, sexually oriented, or threatening materials or messages, whether public or private.

b. Using the network for financial gain or for commercial activity.

c. Attempting to harm or harming equipment, materials, or data.

d. Attempting to send or sending anonymous messages of any kind.

e. Using the network to access inappropriate material.

f. Knowingly placing a computer virus on a computer or the network.

g. Using the network to provide addresses or other personal information that others may use inappropriately.

6. Users will not access information resources, files, or documents of another user without authorization.

7. System users may not disable, or attempt to disable, a filtering device on the District's electronic communications system.

8. Communications may not be encrypted so as to avoid security review by system administrators.

9. System users may not use another person's system account without written permission from the campus administrator or District coordinator, as appropriate.

10. System users must purge electronic mail and data files in accordance with established retention guidelines.

11. System users may not redistribute copyrighted programs or data except with the written permission of the copyright holder or designee. Such permission must be specified in the document or must be obtained directly from the copyright holder or designee in accordance with applicable copyright laws, District policy, and administrative regulations.

12. System users should avoid actions that are likely to increase the risk of introducing viruses to the system, such as opening e-mail messages from unknown senders and loading data from unprotected computers.

13. 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.

14. System users may not waste District resources related to the electronic communications system.

15. System users may not gain unauthorized access to resources or information.

Student Users

Student users must adhere to the standards applicable to all users listed above, as well as the following:

1. Students may not distribute personal information about themselves or others by means of the electronic communications system; this includes, but is not limited to, personal addresses and telephone numbers.

2. Students should never make appointments to meet people whom they met online and should report to a teacher or administrator if they receive any request for such a meeting.

3. Students in grades 6–12 may be issued a filtered email account to use for educational purposes including communication with staff, communication related to assignments, homework or other District projects, higher education admission and scholarship correspondence, and/or other necessary communication related to instructional resources.

Vandalism Prohibited

Any malicious attempt to harm or destroy District equipment or data or data of another user of the District's system or of any of the agencies or other networks that are connected to the Internet is prohibited. Deliberate attempts to degrade or disrupt system performance are violations of District policy and administrative regulations and may constitute criminal activity under applicable state and federal laws. Such prohibited activity includes, but is not limited to, the uploading or creating of computer viruses.

Vandalism as defined above will result in the cancellation of system use privileges and will require restitution for costs associated with system restoration, as well as other appropriate consequences. [See DH, FN series, FO series, and the Student Code of Conduct.]

Forgery Prohibited

Forgery or attempted forgery of electronic mail messages is prohibited. Attempts to read, delete, copy, or modify the electronic mail of other system users, deliberate interference with the ability of other system users to send/receive electronic mail, or the use of another person's user ID and/or password is prohibited.

Information Content / Third-Party Supplied Information	System users and parents of students with access to the District's system should be aware that, despite the District's use of technology protection measures as required by law, use of the system may provide access to other electronic communications systems in the global electronic network that may contain inaccurate and/or objectionable material. A student who gains access to such material is expected to discontinue the access as quickly as possible and to report the incident to the supervising teacher. 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. An employee knowingly bringing prohibited materials into the school's electronic environment will be subject to disciplinary action in accordance with District policies. [See DH]
Participation in Chat Rooms and Newsgroups	Participation in chat rooms and newsgroups accessed via the Internet is permissible for students, under appropriate supervision, and for employees.
District Website	The District will maintain a District website for the purpose of informing employees, students, parents, and members of the community of District programs, policies, and practices. Requests for publication of information on the District website must be directed to the designated contact person. The assistant superintendent for technology services or designee will establish guidelines for the development and format of web pages controlled by the District. No personally identifiable information regarding a student will be published on a website controlled by the District without written permission from the student's parent.
School or Class Web Pages	Schools or classes may publish and link to the District's web pages that present information about the school or class activities, subject to approval from the campus principal. The campus principal will designate the staff member responsible for managing the campus web page [see CQ(EXHIBIT)]. Teachers will be responsible for compliance with District rules in maintaining their class web pages. Any links from a school or class web page to sites outside the District's computer system must receive approval from the campus principal or designee [see CQ(EXHIBIT)].

Extracurricular Organization Web Pages

All District-approved noncurricular clubs or organizations may post student club information on school web pages via a District-provided template. This template will be used to replace all other postings of student club information on school web pages. The template will have the organization/club name, contact person, phone number, description (limited to 15 words or less) and school logo.

Personal Web Pages

District employees, Board members, and members of the public will not be permitted to publish personal web pages using District resources.

Network Etiquette

All system users are expected to observe the following network etiquette:

1. Swearing, vulgarity, ethnic or racial slurs, and any other inflammatory language are prohibited.
2. Pretending to be someone else when sending/receiving messages is prohibited.
3. Submitting, publishing, or displaying any defamatory, inaccurate, racially offensive, abusive, obscene, profane, sexually oriented, or threatening materials or messages either public or private is prohibited.
4. Transmitting obscene messages or pictures is prohibited.
5. Revealing personal information such as addresses or phone numbers of users or others is prohibited.
6. Using the network in such a way that would disrupt the use of the network by other users is prohibited.

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 principal or District coordinator receives notice of student withdrawal or of revocation of system privileges, or on a future date if so specified in the notice.

Consequences of Improper Use

Improper or unethical use may result in disciplinary actions consistent with the existing Student Code of Conduct and, if appropriate, the Texas Penal Code, Computer Crimes, Chapter 33, or other state and federal laws. This may also require restitution for costs associated with system restoration, hardware, or software costs.

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, 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 necessarily 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.

Copyright Compliance

The use of District technology in violation of any law, including copyright law, is prohibited. Copyrighted or licensed software or data may not be placed on any system connected to the District's system without permission from the holder of the copyright or license. Only the copyright or license owner, or an individual the owner specifically authorizes, may upload copyrighted or licensed material to the system.

No person will be allowed to use the District's technology to post, publicize, or duplicate information in violation of copyright law. The technology director will use all reasonable measures to prevent the use of District technology in violation of the law.

Transfer of Equipment to Students

The following regulations will apply to all schools and departments regarding transfer of equipment to students under policy CQ:

1. Proposed projects to distribute equipment to students will be sent to the assistant superintendent for technology services for initial approval.
2. A student is eligible to receive data processing equipment under this regulation only if the student does not otherwise have home access to data processing equipment as determined by the school.
3. In transferring data processing equipment to students, a school will give preference to educationally disadvantaged students as determined by the school.
4. Before transferring data processing equipment to a student, each school must have clearly identified:

a. A process to determine eligibility of students under policy CQ;

b. An application process that identifies the responsibility of the student regarding home placement, use, and ownership of the equipment;

c. A process to distribute and initially train students in the setup and care of the equipment;

d. A process to provide ongoing technical assistance for students using the equipment;

e. A process to determine ongoing student use of the equipment;

f. A process to determine any impact on student achievement that the use of this equipment may provide; and

g. A process for retrieval of equipment from students as necessary.

Accepting Electronic Signatures

The District may accept electronically signed documents or digital signatures for any transactions and purposes allowed by law, including student admissions documents, student grade and performance information, contracts for goods and services, and employment documents. The District will comply with rules adopted by the Texas Department of Information Resources (DIR), to the extent practicable, to:

- Authenticate a digital signature for a written electronic communication sent to the District;
- Ensure that records are created and maintained in a secure environment;
- Conduct risk assessments for transactions involving digital signatures;
- Implement appropriate nonrepudiation services; and
- Maintain all records as required by law.

Note: The "Guidelines for the Management of Electronic Transactions and Signed Records" may be found on the DIR's website.[1]

[1] "Guidelines for the Management of Electronic Transactions and Signed Records": http://publishingext.dir.texas.gov/portal/internal/resources/DocumentLibrary/Texas%20Uniform%20Electronic%20Transactions%20Act%20(UETA)%20Guidelines.pdf