The Superintendent or designee will 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 may provide training to employees, students, and members of the public as needed, scheduled, or requested. Access to the District's system will be granted to users, as required, to participate in educational environments or to complete assigned job duties. Users may access the Technology Acceptable Use Policy and Guidelines online.

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 will be governed by the following.

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

1. Sign the ECISD Employee Handbook Acknowledgment Form.
2. Receive account access from the District's technology department.

Students shall be granted access to the District's system after signing (hardcopy or digitally) the ECISD Student-Parent Handbook Acknowledgment Form.

Members of the public requiring sustained access to District network resources may be granted access after submitting the public (nonschool) user agreement form [CQ(EXHIBIT)] with the person's signature and receiving a final approval and 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. To further 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 will not access a computer account that belongs to another student, employee, or department (except for an authorized member of the District's technology department). Users will 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 and staff data through a District data management application must abide by all federal, state, and local guidelines.
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 IDs, passwords, confidential information, or any file contents (data, video, or audio) on any District computer or network system by staff, 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. Knowingly or recklessly 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 using computer resources, including bandwidth, disk space, printer paper, or running or installing games or other unauthorized software on District's computers, for non-District endorsed educational purposes 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.

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 e-mail messages.

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 websites representing the District or a campus on an outside server.

STAFF RESPONSIBILITIES

Staff must supervise student use of the District's 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 the District's network or equipment to access, transmit, store, display, or request obscene, pornographic, erotic, profane, racist, sexist, terroristic, violent, or other offensive material (including messages, images, video, or sound) that violates the District's harassment policy or creates an intimidating or hostile work or learning 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. General access accounts will be monitored and inappropriate activity will be

addressed in accordance with the ECISD Technology Acceptable Use and Management Guidelines.

6. Teachers are responsible for monitoring all computer use in their rooms, librarians are responsible for all computer use in their library, lab instructors are responsible for all computer use in their labs, campus administrators are responsible for monitoring computer use campus-wide, and department heads are responsible 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 users' 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 whether 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 videotaping 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

The monitoring and use of the District's Voice-over Internet Protocol (VoIP) network will 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 his or her department's web pages. The department head must approve the web pages before they are posted.

6. All department and campus websites must include a hyper 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. Student directory information—student name; photograph; major field of study; degrees, honors, and awards received; dates of attendance; grade level; most recent educational institution attended; participation in officially recognized activities and sports; and weight and height of members of athletic teams—as allowed by the Family Educational Records Privacy Act (FERPA) and identified in policy FL(LOCAL) may be utilized by the District to recognize and promote student achievement.

   A parent or guardian may submit a request in writing to the campus principal or designee and object to use of directory information in accordance with FERPA rules and guidelines.

   The campus principal or designee will be responsible for obtaining the signed release form.

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.