ELECTRONIC COMMUNICATION AND DATA MANAGEMENT

GENERAL DISTRICT RESPONSIBILITIES

The Superintendent or designee will oversee the District's electronic communications systems. Electronic Communication and Data Management includes, but is not limited to online database systems that District personnel use for the data collection and disaggregation of student information, personnel information and finance information.

The District will provide training in the 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

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)E]

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 and District policy. [See CQ(EXHIBIT)F and policies at FL]

FILTERING

Information Technology will 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 on-line gambling.

Portable ECISD computers (laptops, netbooks, etc.) issued to students for use off campus will have the Lightspeed filter client for offsite access installed.

REQUESTS TO DISABLE FILTER

Information Technology staff 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:

Students in grades 3-12 will be assigned individual accounts.

Students granted access to the District's system must complete any applicable District network training.

1. With the completion of District hiring procedures and paperwork, District employees will be granted access to the District's system. Students granted access to the District's system must complete any applicable District network training.

2. The District will require that all passwords be changed every 90 days. All passwords must remain confidential and should not be shared.

3. Any system user identified as a security risk or as having violated District and/or campus computer use guidelines may be denied access to the District's system.

4. All users will be required to sign a user agreement annually for issuance or renewal of an account.

5. Use of home/personal software on ECISD computers is not permitted.

6. Use of home/personal peripherals (printers, tablets, etc.) is not permitted with ECISD computers.

7. Use of home/personal computers is permitted with the following guidelines.

DIRECTOR OF INFORMATION TECHNOLOGY

   a. Personal computers used on ECISD campuses/sites are subject to Electronic Discovery (e-discovery) and Open Records requests. If a request is made, the staff member must provide the computer to the IT department to complete the request.
   b. Personal computers will not access, try to access or have inappropriate material as defined in policy. Computers are subject to investigation at any time by IT staff. If inappropriate material and/or access is discovered, the staff member will be responsible for the content and subject to disciplinary action including possible termination and the computer will be confiscated.
   c. ECISD is not responsible for supporting and maintaining the operation of personal computers. If personal equipment does not work, malfunctions or breaks, ECISD is not responsible for loss of data, damaged/broken equipment or connecting to ECISD equipment (projectors, network, etc.).
   d. Staff are responsible for providing proof of licensing for software and copyrighted material if requested by IT staff.
   e. If the computer is causing problems with ECISD equipment, it will be removed from the campus/site. If ECISD equipment is damaged by staff trying to utilize their personal computer, the staff member will be financially responsible for the damage.

f. ECISD is not responsible for the theft or loss of personal computers on ECISD facilities.

The Director of Information Technology for the District's electronic communications system, or campus designee will:

1. Be responsible for disseminating and enforcing applicable District policies and acceptable use guidelines for the District's system to the campus administrators.
2. Ensure that all software loaded on computers in the District is consistent with District standards and is properly licensed.
3. Ensure that all users of the District's system annually 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 principals or supervisor's office (students) and Human Resources Office (staff).
4. Ensure that employees supervising students who use the District's system provide training, emphasizing the appropriate use of resource.
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 bonafide research or another lawful purpose, based on Information Technology staff recommendation.
7. 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.
8. Set limits for data storage and applications within the District's system, as needed so long as consistent with the Local Government Records Act. [See CPC(Legal)]

SYSTEM ACCESS TO ONLINE DATABASE SYSTEMS

ECISD employees who are granted access to any online database system used for data collection, management and/or disaggregation are held responsible for the professional execution of this access due to the confidential nature of such access. All employees granted this privilege must sign an Online Database Use Agreement and abide by the terms of the agreement. [See CQ(EXHIBIT) G]

INDIVIDUAL USER RESPONSIBILITIES
ONLINE CONDUCT

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

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, personal financial gain or for any other activity prohibited by District policy or guidelines.

3. System users may not use another person's system account without written permission from the staff member's supervisor, as appropriate.
4. System users may not disable, or attempt to disable, or bypass a filtering device on the District's electronic communications system.
5. Students may not distribute personal information about themselves or others by means of the electronic communication system; Includes, but is not limited to, personal addresses and telephone numbers.
6. Students should never make appointments to meet people whom they meet online and should report to a teacher or administrator if they receive any request for such a meeting.
7. System users must purge electronic mail in accordance with established retention guidelines.
8. 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.
9. System users may not send or post messages that are abusive, obscene, pornographic, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.
10. System users may not purposefully access materials that are abusive, obscene, pornographic, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.
11. Communications may not be encrypted so as to avoid security review by system administrators.
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 may download public domain programs for their own use to their computers with completion of the electronic software approval form. System users are responsible for determining whether a program is in the public domain.
14. 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.
15. System users may not waste District resources related to the electronic communications system.
16. System users may not gain unauthorized access to resources or information.
17. System users are subject to the suspension of access to the system, revocation of the computer system account or other disciplinary or legal action.

VANDALISM PROHIBITED

Any malicious attempt to harm or destroy District equipment or data of another user of the District's system or 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, and 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 or 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/or to report the incident to the supervising teacher or campus administrator.

A student knowingly bringing prohibited material into the school's electronic environment will be subject to the suspension of access and/or a 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 policy. [See DH]

PARTICIPATION IN CHAT ROOMS (AND NEWSGROUPS)

No participation in any chat room (or newsgroup) accessed on the Internet is permissible for students or employees.

DISTRICT WEB SITE

The District will maintain a web site 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 Web site must be directed to the designated Webmaster. The Director of Information Technology and the District Webmaster 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 Web site controlled by the District without written permission from the student's parent.

No commercial advertising will be permitted on a Web site controlled by the District.

SCHOOL OR CLASS WEB PAGES

Schools or classes may publish and link to the District's Web site pages that present information about the school or class activities, subject to approval from the Webmaster. The campus principal will designate the staff member responsible for managing the

campus's Web page under the supervision of the District's Webmaster. 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 will be subject to review by the District Webmaster.

EXTRA-CURRICULAR ORGANIZATION WEB PAGES

With the approval of the District Webmaster, extracurricular organizations may establish Web pages linked to a campus or District Web site; however, all material presented on the Web page must relate specifically to organization activities and include only student-produced material. The sponsor of the organization will be responsible for compliance with District rules for maintaining the Web page. Web pages of extracurricular organizations must include the following notice: "This is a student extracurricular organization Web page. Opinions expressed on this page shall not be attributed to the District." Any links from the Web page of an extracurricular organization to sites outside the District's computer system will be subject to review by the District Webmaster.

PERSONAL WEB PAGES

District employees, Trustees, students and members of the public will not be permitted to publish personal Web pages using District resources.

NETWORK ETIQUETTE

System users are expected to observe the following network etiquette:

1. Be polite; messages typed in capital letters are the computer equivalent of shouting and are considered rude.
2. Use appropriate language; swearing, vulgarity, ethnic or racial slurs, and any other inflammatory language are prohibited.
3. Pretending to be someone else when sending/receiving messages is considered inappropriate.
4. Transmitting obscene or threatening messages or pictures is prohibited.
5. Be considerate when sending attachments with e-mail by considering whether a file may be too large to be accommodated by the recipient's system or may be in a format unreadable by the recipient.
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

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 Director of Information Technology receives written notice of student withdrawal or of revocation of system privileges, or on a future date if so specified in the notice.

The District's system is provided on an "as is, as available" basis. The District does not make any warranties, whether expressed 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 the functions or services performed by, or the information or software contained within will meet the system user's requirements. The District furthermore does not warrant the system will be uninterrupted or error-free, or the 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 communication 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 submit licensed or copyrighted material to the ECISD networking team for approval to be uploaded 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 Director of Information Technology will use all reasonable measures to prevent the use of District technology in violation of the law.

COMPLAINTS REGARDING COPYRIGHT COMPLIANCE

If a copyright or license owner reasonably believes that the District's technology has been used to infringe upon a copyright or license, the owner is encouraged to notify the District.

The District designates the following employee to receive any complaints that copyrighted material is improperly contained in the District network:

Name: Information Technology Designee
Position: Webmaster