

Administrative Regulation

Electronic Communication And Data
Management (REGULATION)

CQ
(Regulation)

	<p>The Superintendent or designee will oversee the District's electronic communications system.</p> <p>The District will provide training in proper use of the system and will provide all users access to the acceptable use guidelines. All training in the use of the District's system will emphasize the ethical and safe use of this resource.</p>
Acceptable Use Policy	<p>The Superintendent of Laredo Independent School District has delegated the responsibility of the development, revision and implementation of the District's Acceptable Use Policy to the Chief Technology Officer. Laredo Independent School District employees are responsible to act in accordance with these policies and procedures.</p>
Filtering Policy	<p>The Superintendent of Laredo Independent School District has delegated the responsibility to the Chief Technology Officer of maintaining an appropriate filtering policy in our District that will comply with the Children's Internet Protection Act. (CIPA) All Internet access will be filtered for minors and adults on computers with Internet access provided by the school.</p> <p>The Chief Technology Officer or designee will consider requests from users who wish to use a blocked site for bona fide research or other lawful purposes.</p>
System Access	<p>Access to the District's electronic communications system will be governed as follows:</p> <ol style="list-style-type: none">1. Employees and students, in grades Pre-K thru 12th, will be granted access to the District's system as appropriate.2. No students in grades Pre-K thru 1st will be assigned an individual account or password.3. Students in grades 2nd thru 12th will be assigned individual accounts if parents grant permission.4. Employees/Students granted access to the District's system must complete any applicable District network training.5. As appropriate and completion of District network

training, District employees/students will be granted access to the District's system.

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

7. All users will be required to agree to the District's Acceptable Use Policy annually for renewal of an account.

Technology Coordinator/Director Responsibilities

The Technology Director or designee for the District's electronic communications system 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 complete and sign an agreement to abide by District's Acceptable Use Policy 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 safety online and proper use of the system.

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

Individual User Responsibilities for 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, or for any other activity prohibited by District policy or guidelines.

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

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

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

6. 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.

7. 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.

8. System users must purge electronic mail in accordance with established retention guidelines.

9. 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.

10. 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.

11. System users may not send or post messages that are abusive, obscene, pornographic, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.

12. 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.

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

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

15. Users accessing District resources via Personal Telecommunications/Electronic Devices (PTEDs) must also adhere to all policies applicable to District owned technology equipment.

16. Limited personal use of the system shall be permitted if the use: 1) imposes no tangible cost on 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.

Vandalism & Forgery Prohibited

Any malicious attempt to harm or destroy District equipment or data or the 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 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]

District Web Site

The Communications Department will maintain a District 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 Communications 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.

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. 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 must receive approval from the District Webmaster or designee.

With the approval of the District Technology Director or

designee, students may establish individual Web pages linked to a campus or District Web site; however, all material presented on a student's Web page must be related to the student's educational activities. Student Web pages must include the following notice: "This is a student Web page. Opinions expressed on this page shall not be attributed to the District." Any links from a student's Web page to sites outside the District's computer system must receive approval from the District Webmaster.

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 must receive approval from the District Webmaster.

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

Network Etiquette

All users are expected to use the network and its resources in a polite and ethical manner. Activities contrary to this include but are not limited to:

- Users sending messages or images that can be considered rude or obscene.
- Users impersonating other users.
- Users wasting District resources.
- Users using the network in such a way that disrupts other users from using the network.

Termination/Revocation Of System User Account 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 Technology Coordinator/Director receives notice of student withdrawal or of revocation of system privileges, or on a future date if so specified in the notice.

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.

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 coordinator/director 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: Veronica Castillon

Position: Director of Communications

Address: 1702 Houston Street

Telephone: (956) 273-1730

E-mail: vcastillon@laredoisd.org

The Superintendent or designee will register this information with the federal Register of Copyrights, in accordance with federal requirements.

Issuance of Technology
Equipment to Students

The following rules will apply to all campuses and departments regarding transfer of computer equipment to students under provisions of law cited at CQ(LEGAL):

1. Proposed projects to distribute computer equipment to students must be submitted to the Director of Technology for initial approval.
2. Before issuing computer equipment to a student, the technology director must have clearly outlined:
 - a. A process that identifies the responsibility of the student regarding proper use, both at home and at school, of the technology equipment.
 - b. A process to distribute and initially train students in the setup and care of the equipment;
 - c. A process to provide ongoing technical assistance for students using the equipment;
 - d. A process for retrieval of the equipment from a student, as necessary.

9/11/2013
Date Approved
9/16/2013
Date Approved
9/18
Date Approved

Elizabeth J. Jarama
Director for Instructional Technology
[Signature]
Chief Technology Officer
[Signature]
Superintendent