Acceptable Use Policies and Guidelines

LAREDO INDEPENDENT SCHOOL DISTRICT

Revised: April 2018

Laredo Independent School District
Board of Trustees

Members:
Hector J. Garcia - District 6, President
Hector J. Noyola – District 3, Vice-President
Ricardo Garza – District 4, Secretary
Jose A. Valdez - District 1, Trustee
Cindy Liendo – District 2, Trustee
Dr. Cecilia May Moreno – District 5, Trustee
Jose R. Perez – District 7, Trustee

Superintendent of Schools
Dr. Sylvia G. Rios

Technology Educational Goals

(Technology Plan, 2013 - 2016)

- **Goal 1: Teaching and Learning - LISD will provide technology resources for educators to deliver instructional content through the use of technology tools, resources and services in order to seamlessly integrate technology to all curricular areas.**
  - **Objective 1.1:** LISD teachers and staff will implement research-based strategies to improve academic achievement, evident in student achievement data across all content areas and technology literacy data.
  - **Objective 1.2:** All LISD teachers will integrate the Technology Applications TEKS within the foundation curriculum at each grade level K-8th and LISD high schools will offer Technology Applications courses as an option.
  - **Objective 1.3:** All teachers and administrative staff will use student performance data (from district/state assessment instruments) with electronic curriculum resources to inform and differentiate instruction for every child.
  - **Objective 1.4:** LISD will ensure that all school libraries have the latest technology and online resources for student research and curriculum integration.
  - **Objective 1.5:** Each campus will implement an innovative program that promotes parental involvement, increased communication with parents and community members and community access to educational resources.

- **Goal 2: Educator Preparation and Development - LISD will provide professional development in technology which has been correlated to the SBEC technology standards.**
  - **Objective 2.1**: LISD's will provide professional development for teaching and integrating Technology Applications into the foundation and enrichment TEKS through multiple delivery methods year-round.
  - **Objective 2.2:** LISD's Technology Department will promote technology proficiency levels and strategies for all educators, including campus administrators and librarians to ensure higher levels of technology implementation.
  - **Objective 2.3:** LISD will provide campuses access to an Instructional Technology Trainer to be used as coaches and mentors to support classroom efforts in using technology to improve learning in core curriculum areas.

- **Goal 3: Leadership, Administration and Support - LISD will work on integrating technology programs into teaching and learning and into all departments to improve effectiveness and efficiency, to develop technology savvy leaders, and provide technical and instructional technology support staff.**
  - **Objective 3.1:** LISD staff will identify budget and secure funding to support technology identified in all classroom, libraries, campus, and district planning efforts.
  - **Objective 3.2:** LISD will implement a plan to employ additional staff to meet the one technician for every 350 computers as stated in the STaR Chart.

- **Goal 4: Infrastructure for Technology - LISD will provide a secure, cost efficient technology infrastructure for every student and staff member with direct connectivity available in all rooms and web-based resources in multiple rooms.**
  - **Objective 4.1:** LISD will apply with The Schools and Libraries Program of the Universal Service Fund (erate) for discounts available on telecommunication services, Internet access, and internal connections.
  - **Objective 4.2:** LISD will strive to achieve and maintain a lower personal computing ratio for both students and professional educators.
  - **Objective 4.3:** LISD's Technology and Communication departments will provide and maintain an infrastructure for communication with parents and community members, including year-round access to school news, educational resources, data and personnel.

User's Guidelines

Purpose and Availability of Access

All district guidelines and procedures for acceptable use of technology are intended to make the district's technology equipment, applications/programs and the system network more efficient, accessible and reliable for all *"*users.*"*

"User" is defined as Laredo ISD students, employees, volunteers, community members, and guests (including vendors' representatives and consultants, service providers, and employees of subcontracted companies) with access to a computer, Internet, and other technological equipment and software through the district.

To prepare students for an increasingly computerized society and facilitate employee work productivity, the district has made a substantial investment in providing its students and employees access to the Internet, computing equipment, systems and local network functions. Use of these resources is 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 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.

The use of the district's technology equipment and the participation in any online communication services (i.e. Internet, e-mail, distance learning and Intranet, etc.) **is a privilege and not a right.**

Personal Telecommunications/Electronic Devices (PTED)

Students and employees in our district have personally owned technologies readily available to them. These devices include but are not limited to smart phones, tablets (iPads and Windows tablets, etc.), electronic readers (Nook, Kindle, etc.), netbooks, etc. These items are generally referred to as "Personal Telecommunications/Electronic Devices" (PTEDs). PTEDs using or accessing district resources (i.e. WiFi) are subject to the same Acceptable Use Policies (AUPs) listed throughout this manual unless otherwise stated. Furthermore, the IT Department does not address any technical issues related to PTEDs. Maintenance and troubleshooting of PTEDs is solely the responsibility of the student or employee possessing the device. The district is not responsible for loss, theft and/or damages to PTEDs brought into the district.

All users shall be required to acknowledge receipt and understanding of all administrative regulations, Acceptable Use Policies and shall agree in writing to allow monitoring of their use and to comply with such regulations and guidelines. Students under age 18 will require parental permission.

Noncompliance with applicable regulations and guidelines will result in disciplinary action consistent with district policies and regulations. (See LISD Student Code of Conduct, and Local DH Code of Ethics and Standard Practice for Texas Educators, Regulations) Violations of law may result in criminal prosecutions as well as disciplinary action by the district.

Audits and monitoring

User shall understand LISD has the right to periodically audit, inspect, and/or monitor all use of LISD technology, PTEDs when deemed appropriate and/or arbitrarily. This includes the access to resources, remote and local.

Audits – Electronic auditing shall be implemented within all unclassified networks that connect to the Internet or other publicly accessible networks to support identification, termination, and prosecution of unauthorized activity. These electronic audit mechanisms shall be capable of recording:

- Access to the system, including successful and failed login attempts, and logouts;
- Inbound and outbound file transfers;
- Terminal connections to and from external systems;
- Sent and received e-mail messages;
- Web sites visited;
- Date, time and user associated with each event;
- Access to remote desktops;
- Downloaded material, including files deleted from a user's account.

Filtering

Laredo ISD will abide by the Children's Internet Protection Act of 2001 (CIPA). Filtering policy is reviewed on an annual basis by the Technology Department. Specifically, these criteria will be followed:

1. Filtering will be provided for all Internet enabled computers used by students, patrons, and staff
2. Requiring PTEDs to log onto the district's network when accessing or using district resources to enable filtering.
3. Filtering will be disabled only for bona fide research or other lawful purposes
4. Online activities of minors will be monitored for appropriate use
5. Safe and secure use by minors of direct electronic communications will be assured
6. Unauthorized disclosure, use and dissemination of personal identification information regarding minors are prohibited.

Family Educational Rights and Privacy Act (FERPA)

Laredo Independent School District will comply with all FERPA requirements as it pertains to the protection of the privacy of student educational records. (20 U.S.C. § 1232g; 34 CFR Part 99).

FERPA gives parents and students 18 years of age or older the right to review and inspect student records and request amendments to the record if they feel the information is misleading. Requests for amendments are subject to review by the district and can be granted or denied. Parents and eligible students have the right to a formal hearing if the decision was not to their satisfaction.

In most cases, parent or eligible student written permission is needed in order to release any information in student's educational record. There are some instances where parental permission is not required.

The following is a list of those exceptions (34 CFR § 99.31):

- School officials with legitimate educational interest;
- Other schools to which a student is transferring;
- Specified officials for audit or evaluation purposes;
- Appropriate parties in connection with financial aid to a student;
- Organizations conducting certain studies for or on behalf of the school;
- Accrediting organizations;
- To comply with a judicial order or lawfully issued subpoena;
- Appropriate officials in cases of health and safety emergencies; and
- State and local authorities, within a juvenile justice system, pursuant to specific State law.

Any LISD employee accessing student educational records is required to follow these guidelines. If a request is made by a vendor or outside entity for student educational records, the employee must refer them to the Communications Department.
Any employees who receive student educational records in error must report it immediately to the Communications Department.

District Technology Equipment Usage

Defining Technology Equipment Usage Rights/Purposes

All Laredo Independent School District's technology equipment inclusive of internal, external or online storage devices and related media is to be used for school business (instructional and administrative purposes). Instructional purposes include any activities that support the district's instructional goals and objectives.

LISD will not be responsible for the loss of any files on district technology equipment and it is the user's responsibility to save/backup all resources to an external or online storage medium.

Laredo ISD computers require a windows login and password to access to computer/network resources. User is responsible to log out at the conclusion of his/her use of the equipment.

Acceptable Conduct

1. Users shall protect the security and privacy of LISD's systems and network.
2. Users shall treat technology equipment with care. Information on proper care is provided by the Instructional Technology Department upon request.
3. Users who check out technology equipment/software shall be responsible and must make sure that equipment is operating properly prior to being checked out. It is also the responsibility of the user to return the technology equipment/software in the same condition it was checked out. (normal wear and tear accepted).
4. Users shall obtain permission before opening, moving, deleting, or duplicating the computer files of others.

Limitation of Uses

1. Users shall not hack or otherwise alter programs or files belonging to other users.
2. Users shall not take actions that are harmful to the district's technology equipment (vandalism).
3. Users shall not remove any district technology equipment from US boundaries.
4. Users shall not use the computer/technology equipment in any way that may harass, defame or demean others with language, image or threats.
5. Users shall not use computer/technology equipment for personal use such as for commercial purposes, financial gain, advertisement, and seeking/interacting with professional unions, political lobbying, and supporting illegal activities.
6. Users shall not use/download any non-educational file sharing sites or resources.
7. Users shall not make any changes to the computer/technology equipment configurations (i.e. network settings).
8. Users shall not use unauthorized administrative logins and passwords without the written approval from the Director of Instructional Technology or Chief Technology Officer.
9. Users shall not write, produce, generate copy, propagate, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of any computer's memory, file system, or software. Such software is often called a bug, virus, worm, Trojan horse, or similar name.
10. Users shall not assemble or disassemble computers/technology equipment without written permission from Director of Instructional Technology or Chief Technology Officer.
11. Users shall not move computer/technology equipment from designated areas without the written permission of the Technology Trainer or Campus/District Administrator. (An Inventory Transfer Form must be completed and turned in to campus designee before move is made.)
12. Users shall not misuse district resources. (i.e. paper, toner, disk space (storage of video or music))
13. Users shall not use district equipment (laptops, desktops or telecommunication/electronic devices) to access social networking sites for personal non-educational reasons (i.e. Facebook, Twitter, Instagram, YouTube).

District Software Usage

Software Purchases/Installation/Usage

All software purchase or acquisitions must follow outlined district guidelines.

- All software must first be approved by the Curriculum and Instruction Department for content then by the Information or Instructional Technology Department so that it may be checked for compatibility with district technology equipment before purchase. A pilot of the installation may be required in order to check compatibility.
- After software arrives, a work order must be filled out for installation to occur. Work order must contain all pertinent details including room number and identification of computers requiring installation. Work order must also include the PO# (of the software purchase) to verify the number of licenses purchased.
- The IT department or designee will perform installation.
- Software may not be purchased solely for individual use unless approved by the Curriculum and Instruction Department.

- District technology staff has the right to remove any unauthorized software on any district/campus technology equipment.
- LISD prohibits the use of games for staff and students with the exception of educational software that has been approved by the district.
- LISD prohibits the use of unauthorized access points or satellite software, which can access LISD's network. Chief Technology Officer must approve all such technology equipment and software before purchase is made.

Acceptable Conduct

1. Users who record student attendance will annually certify in writing that all such records are true and correct to the best of his or her knowledge and that the records have been prepared in accordance with laws and regulations pertaining to student attendance accounting.
2. Users shall input correct and true data to the best of his or her knowledge.

Limitation of Uses

1. Users may not install any type of software, demos, files, or plugins. If any of these are needed, a work order for the installation must be completed at the campus/department level.
2. Users shall not transmit files that contain software or other material protected by intellectual property laws, rights of privacy of publicity, or any other applicable law unless user owns or controls the rights thereto or has received all necessary consents.
3. Users shall not act, or fail to act, in use of software, in a manner that is contrary to applicable law or regulation.
4. Users shall not falsify the source or origin of software or other material contained in a file that is transmitted.
5. User shall not install or run any executable files (.exe, .bat, .com) that can render a computer as a network device. Installing this type of software creates network traffic or shares and is not allowed.
6. Users shall not misuse, falsify or share confidential data including but not limited to the following: Sage/ALIO, SchoolMax, PEIMS, DMAC, TREx, PID/P.E.T.

Internet Usage

Defining Internet Usage Rights/Purpose

LISD is providing access to the Internet with the purpose to facilitate teaching and learning of the curriculum in accordance with Laredo ISD educational objectives. Therefore, Internet users must restrict their activities to endeavors in support of district educational and administrative objectives. In accordance with the appropriate certification, the district shall monitor the on-line activities of minors including activity on PTEDs. 47 U.S.C. 254(h)(5)(B) [CQ Legal]

In accordance with the appropriate certification, the district operates 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) (Board Policy – CQ Legal)

The district uses Internet content management software to filter content and sites that are considered inappropriate. This software allows the district to run reports detailing all activity on individual accounts. The district has the right to generate a User Access Report detailing all violations. A report will be generated if the user is or is suspected of abusing the privilege of Internet access, violating any of the guidelines, or misusing the Internet.

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. *(Local regulation CQ)*

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. The individual in whose name a system account is issued will be responsible at all times for its proper use. *(Local regulation CQ)*

The following procedures will be applied at all campuses and departments:

1. At the campus, the classroom teacher with or without the assistance of the Technology Trainer will provide training in the proper use of the system and ethical and safe use of this resource. Teacher will provide all users the online link to these guidelines for further reference. All training in the use of the district's system will emphasize the ethical and safe use of this resource. Training will also focus on cyber-bullying and ways students can prevent their exposure to online predators.(Local regulation CQ).
   At the departments, the district assigned trainer will provide training in the proper use of the system and ethical and safe use of this resource. Trainer will provide all users the online link to these guidelines for further reference. All training in the use of the district's system will emphasize the ethical and safe use of this resource. *(Local regulation CQ)*
2. After the training, the students/staff will be given a form to sign that they will abide by these AUPs. Students under 18 years of age will require for parent(s) to sign form.
3. Completed forms need to be turned in to the homeroom teacher so account may be activated. Account logins will be issued to each student who has completed training and turned in signed required forms.

Acceptable Conduct

1. Users shall use the Internet for educational and administrative purposes and as a tool to enhance teaching and learning in the classroom.
2. User level passwords (e.g., e-mail, web, desktop computer, etc.) must be changed at least every six months.
3. All passwords must remain confidential and should not be shared. *(Local regulation CQ)*
4. Users will be required to sign a user agreement annually for issuance or renewal of an account. All such agreements will be maintained on file electronically in the principal or supervisor's office. *(Local regulation CQ).*
5. Users shall use Internet resources in accordance with copyright law. Copyright is implied in all cases whether or not explicit reference to copyright is mentioned.

6. Users shall use the Internet in accordance with civic and federal laws.
7. Users who gain access to inappropriate material are expected to discontinue the access as quickly as possible and to report the incident to the supervising teacher/supervisor. *(Local regulation CQ)*
8. Users shall conserve district resources (paper in printer, disk space, bandwidth, etc.).

Limitation of Uses

1. Users shall not use the Internet for non-educational purposes. 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. *(Local Regulation CQ)*
2. Users may not disable, or attempt to disable, a filtering device on the District's electronic communications system. *(Local regulation CQ)*
3. Users shall not encrypt communications so as to avoid security review by system administrators. *(Local regulation CQ)*
4. Users shall not use student's/staff system account without written permission from the campus administrator or Technology Director/Coordinator, as appropriate. *(Local regulation CQ)*
5. Users shall not use or 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. Users will be held accountable for the use of copyright protected material obtained from third parties in the case where these parties are in violation of copyright law. *(Local regulation CQ)*
6. Users may not use the Internet to gain unauthorized access to resources or information. *(Local regulation CQ)*
7. Users shall not use the Internet unless they have received training, returned the appropriate agreement form signed and parents have agreed to allow use of the Internet.
8. Users shall not distribute personal information about themselves or others through the Internet. (Local regulation CQ)
9. Users shall not maliciously attempt to harm or destroy district technology equipment or data, or the equipment or data of any of the agencies or other networks that are connected to the Internet. (Local regulation CQ)
10. Internet users shall not purposefully access or post materials that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's image or illegal. (Local regulation CQ) These items include but are not limited to the following categories:
    a) Sites with images or text that is provocative, suggestive and/or erotic in nature.
    b) Sites that promote activities which are illegal for minors (such as drinking alcohol)
    c) Sites that contain content a "reasonable person" may find repulsive or disgusting.
    d) Sites that promote criminal activity. Examples include but are limited to:
        - Building bombs or explosives
        - Hacking into computer systems
        - Lock picking
    e) Sites that promote the use of illegal controlled substances or instruct the reader how to grow/make/process these substances.
    f) Sites that allow the playing or downloading non-educational games.

g) Sites that allow on-line gambling or are dedicated to gambling information and instructions.
h) Sites that advocate intolerance or hatred of a person or group of people (gangs).
i) Sites that show or advocate violence. Examples include: Images containing graphic violence (blood/murder), promotion of violence or terrorist acts against others.

11. Users are prohibited to bring prohibited materials into the school's electronic environment. (Local regulation CQ)
12. Users shall not access or post any information that is confidential or proprietary about the district, and should not communicate with students who are currently enrolled in the district on any social networking sites such as but not limited to Facebook, Twitter, and Instagram unless deemed for educational purposes or if the students are kin to the user.
13. Users shall not participate in any use of the Internet in any way that may harass, defame, or demean others with language, or images that harass, threaten, torment, taunt, stalk, humiliate, coerce or intimidate others. Such actions are classified as cyber-bullying and are a direct violation of the district's electronic policy.
14. Users shall not participate in blogs, newsgroups or chat rooms in a non-educational manner. With approval from the Instructional Technology or the Curriculum and Instruction Department, blogs, chat rooms and newsgroups can be made available for educational use.

Electronic Mail Usage

Defining Certain Rights/ Purpose

The purpose of the school district's e-mail is to facilitate communications in support of research and education. **Access to the district's e-mail system is a privilege, not a right.** Users of the district e-mail system are required to comply with all district rules, regulations, and policies governing appropriate use of the 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.
- Parents have the right to request copies of e-mail sent or received by their daughter/son.
- Supervisors have the right to request copies of e-mail sent or received by staff if suspicion concerning inappropriate use exists.

Acceptable Conduct

1. Users shall use e-mail for educational purposes and must be consistent with the educational mission of the Laredo Independent School District.
2. Users must purge electronic mail in accordance with established retention guidelines to ensure proper use of system. *(Local regulation CQ)*
3. Users shall report illegal or unauthorized use of the e-mail or online systems to the Technology Trainer and/ supervisor.
4. Users are expected to observe the following network etiquette: *(Local regulation CQ)*

- Be polite; messages typed in capital letters are the computer equivalent of shouting and are considered rude.
- Use appropriate language; swearing, vulgarity, ethnic or racial slurs and any other inflammatory language are prohibited.
- Pretending to be someone else when sending/receiving messages is considered inappropriate.
- 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.

Limitation of Uses

1. Users shall not use the e-mail system for any illegal activity, including but not limited to violation of copyright laws (plagiarism, forgery or attempted forgery of electronic mail messages). *(Local regulation CQ)*
2. Users shall not share their login or password with anyone. *(Local regulation CQ)*
3. Users shall not forward district e-mail to their personal e-mail account.
4. Users may not transmit/distribute personal information about students by means of the electronic communications system; this includes, but is not limited to, personal addresses and telephone numbers**.** *(Local regulation CQ)*
5. Users 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. *(Local regulation CQ)*
6. Users shall not use e-mail to sell or to solicit products or services. Users shall not use e-mail for private or commercial offerings of products or services.
7. Users shall not use and/or respond to e-mail in any way that would be considered:
    1) Damaging to another's reputation
    2) Abusive
    3) Obscene
    4) Sexually oriented
    5) Offensive
    6) Threatening
    7) Harassing
    8) Illegal
    9) Contrary to school policy. (Local regulation CQ)
8. Users shall not attempt 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. (Local regulation CQ)
9. Users shall not use the e-mail system to distribute material or information on behalf of or with regard to professional unions, collective bargaining, private businesses or associations, or political campaigns or organizations without the express written consent of the Superintendent or designee.
10. Users shall not access private e-mail accounts such as **HOTMAIL, YAHOO MAIL,** etc. when using the district's Internet system.
11. User shall not use e-mail for the purpose of sending unnecessary or junk mail or chain letters.
12. Users shall not respond to unsolicited e-mail messages from any source without the permission of the supervising teacher.

13. User shall not pretend to be someone else when sending/receiving messages.
14. Users shall not use e-mail for any purposes that may present a tangible cost to the school or interfere with the operations of the computer network or with the performance of the student or employees.

Developing and Publishing of Web Pages

Defining Web Pages Usage Rights/Purposes

Web sites should be primarily academic in nature. They may also serve to support our educational programs by informing our community about events and activities and reflect the unique personality of each school. Users should be mindful that publishing a web page on LISD's web server might cause some recipients or other visitors of that web site to assume they represent the district or school, whether or not that was the user's intention. LISD defines "web page" as any web accessible file or class page that is published to a district funded web site regardless of file type or server location.

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 Webmaster. The Communications Department and the District Webmaster will establish guidelines for the development and format of web pages controlled by the district. (Local regulation CQ)

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.

No commercial advertising will be permitted on a website controlled by the district unless it is placed there by district's Webmaster with administrative approval. (Local regulation CQ)

1. Web pages and web page content created by employees belong to the district even if the employee is no longer in the district.
2. The district has the right to deny publishing a school's or a department's web page that does not follow the approved districts web page template.
3. The district's webmaster or campus website manager has the right to delete any web page that uses excessive system resources or network bandwidth or that is in violation of any of the guidelines outlined below.
4. Roles and responsibilities of the developers in the web page creating/posting process:
    a. Campus Site Manager: The site manager is expected to facilitate all site administrator assignments and provide necessary training for campus site administrators.
    b. Campus Site Administrator(s): Faculty member(s) assigned site privileges/permissions to manage user accounts, class pages, group pages, site announcements, site calendars, and other site resources.
    c. Classroom Teacher: Each classroom teacher should develop and maintain a class page to share class materials, resources, and schedules on the Internet. Class pages should be developed according to current district approved template and should provide resources relevant to grade and subject areas.

d. Group Page Manager: Faculty or student designated to maintain a group page to share files, establish online discussion boards, schedules and other site resources among group members. Group pages may be developed for academic departments, administrative departments, and extracurricular activities.

Acceptable Conduct

1. Users shall publish school-related web pages. Web page content and the intent shall be in accordance with the Laredo Independent School District's Internet policies and guidelines.
2. Users of web pages shall be in compliance with federal copyright laws.
3. Users shall obtain permission from originator in order to publish information, graphics or photographs on any school related web page. All graphics, photos, and art must include site references.
4. Users' web pages shall be appropriate in relation to the objectives of the class/campus/district.
5. Users, who publish a *school-related* web page on the Internet, shall use only the campus/district's web servers to publishing their WebPages.

Limitation of Uses

1. Users shall not use excessive resources on web pages.
2. Users shall not create campus and departments' web pages without using the district's approved template. Teachers and students individual web pages do not need to follow the approved district's web page.
3. Users shall not publish web pages for commercial or private advertising, commercial offerings of products or services for sale, or solicit products or services or to raise funds for non-district related activities or organizations.
4. Users of web pages shall not use the network to disseminate material or information on the behalf of or with regard to professional unions, collective bargaining, private businesses or associations, or political campaign organizations without the express written consent of the Superintendent.
5. Users who create *school-related* web pages **shall not publish their work outside of the districts web server**. (i.e. local provider, geocities.com, etc)
6. Users cannot post any personally identifiable information about a district student 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 A) and policies at FL]
7. Users shall not identify students on school's web pages. Users shall follow these guidelines:
    a. When appropriate, first initials and last names or first name along with initial of last name shall be used. Complete first and last name can be listed with parent permission.
    b. Student work shall not reveal family or personal details that may be construed as invasion of privacy for student or family members.
    c. Student pictures shall not be published unless written parental permission or student (for students over 18 years of age) permission is obtained.

Distance Learning/Videoconference Usage

Defining Certain Rights/Purposes

Distance Learning is two-way communication between a teacher and student separated by distance, using technology for facilitating and supporting the curriculum. Videoconferencing is one form of distance learning where two or more distant groups communicate "face-to-face", in real time, by using audio and video equipment. It brings people in one location together with those in another-whether it is from a university to a medical institution or from a middle school to a library-allowing them to share their knowledge, experiences, and backgrounds.
Note: 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's system is provided on an "as is, as available" basis. The district does not make any warranties, whether express of 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 interrupted or error free or that defects will be corrected.

Acceptable Conduct

1. Users shall be observant that the use of school-related videoconference system might cause some recipients to assume they represent the district or school, whether or not that was the user's intention.
2. Users (students) shall follow all rules as specified by the teacher.

Limitation of Uses

1. Users shall not use the system in any way that violates copyright laws. Users must have permission from the owner of the copyright to use copyrighted materials during the videoconference.
2. Students must have parental consent to participate in videoconferences.
3. Any original work created by users shall not be included in a videoconference session under the district's control unless the district has received written consent from the student and the student's parent.

Non-Employee Equipment/Accessories on LISD Network

Any technology equipment that is not LISD property may not be used in the Laredo ISD network/premises until cleared through the IT Department.

Vendors, consultants and representatives may be allowed to use their own equipment if they have been given proper authorization by the IT Department.

Disciplinary Action

Students and staff must follow all district's AUPs when using district computers/technology equipment or when participating in a school-related activity.

Violations of the Student Code of Conduct with the use of district's computers and networks will result in disciplinary action as stated in the Student Code of Conduct Handbook.

The severity of the violation committed using technology will result in the degree of disciplinary action.

Deliberate attempts to degrade or disrupt system performance are violations of the District's Acceptable Use Policies and may constitute criminal activity under applicable state and federal laws. The district will cooperate fully with local, state, and federal officials in an investigation concerning or relating to the misuse of any electronic communication and data management system. (Local regulation CQ)

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]

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. (Local regulation CQ)

The user causing the system's damage must reimburse any costs that the district incurs due to the misuse or abuse of the system.

Level I Violation/Offense

Any violations of the limitations of usage within these guidelines will be considered a Level 1 violation; unless the violation is classified as a Level II or III violation.

Recommended Consequences for Level I Violation/Offense

Student Offenders

These offenses are prohibited at school or school-related activities and may be punishable by in school suspension, detention, Saturday school, assignment of school duties other than class tasks, withdrawal of extracurricular or honorary privileges, or any other discipline management techniques listed in Section III of the Code, as determined by the campus principals.

District Staff Offenders

Please contact the Human Resources Department to discuss consequences of violation. Generally, the district uses a progressive employee discipline system.

This involves giving the employee a verbal warning for a first offense and a written reprimand for the second. Third violations are treated on a case-by-case basis. However, if the violation is severe, the employee may be suspended and dismissed for cause without resorting to progressive discipline.

Level II Violation/Offense

The following violations are immediately considered level II offenses.

- Take actions that are harmful to the district's technology equipment (vandalism).
- Use the computer/technology equipment in any way that may harass, defame or demean others with language, image or threats.
- Attempt to use or discover any password used for administrative software and hardware to gain illegal entry.
- Write, produce, generate copy, propagate, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of any computer's memory, file system, or software. Such software is often called a bug, virus, worm, Trojan horse, or similar name.
- Assemble or disassemble computers/technology equipment without written authorization from the Information or Instructional Technology Director.
- Malicious attempts to harm or destroy district technology equipment or data, or the equipment or data of any of the agencies or other networks that are connected to the Internet.
- Purposely access or post materials that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's image, or illegal. These items include but are not limited to content filtering software categories under the Internet Usage section (Limitations of usage, #7).
- Say, send, post messages, or use hand gestures that are abusive, obscene, sexually oriented, threatening, harassing, or damaging to another's reputation which using the video conferencing equipment.
- Hack or alter programs or files belonging to other users. For example, erasing, renaming, or making unusable anyone else's files, programs, email or disks.
- Knowingly bringing prohibited materials into the school's electronic environment

Recommended Consequences for Level II Violation/Offense

Student Offenders

These offenses constitute "serious misbehavior" where that term appears in the Code of Conduct. These offenses are prohibited at school or school-related activities and will be punishable by suspension, detention, in-school suspension, Saturday school, assignment of duties other than class tasks, withdrawal of extracurricular or honorary privileges, or any other discipline management techniques listed in Section III of this Code, as in Section II of this Code. Thus, in most cases, the offenses listed in this section will warrant greater consequences than those listed in Level I Minor Offenses section. (Example: serious offenses should warrant a greater number of days spent in in-school suspension than minor offenses.

In some cases, the offenses listed in this section may also meet the definition of conduct, which warrants Discipline Alternative Education Program (DAEP) placement. For instance some of the offenses listed in this section also constitute "engaging in conduct that is punishable as a felony," which is a mandatory DAEP offense. Additionally, some of the offenses listed in this section (depending on the nature and severity of the incident in question) might be considered so severe that they constitute conduct that "substantially

interferes with the orderly operation of the campus" or with the "teacher's ability to communicate effectively." If this occurs, the offense in question is elevated to a Level III offense, and the campus administration may consider DAEP placement.

For those students who are already in the Discipline Alternative Education Program (DAEP), the offenses listed in this section may be grounds for expulsion.

District Staff Offenders
Please contact the Human Resources Department to discuss consequences of violation. Generally, the district uses a progressive employee discipline system.

This involves giving the employee a verbal warning for a first offense and a written reprimand for the second. Third violations are treated on a case by case basis. However, if the violation is severe, the employee may be suspended and dismissed for cause without resorting to progressive discipline.

Reimbursement must be made for any costs that the district incurs due to the misuse or abuse of the system. Authorities may be notified at administrators' discretion. All possible legal actions will be taken against offenders. [See Policy DH]

Level III Violation/ Offense

These offenses are considered to be more serious than the Level II Serious Offenses listed in this Code.

Recommended Consequences for Level III Violation/Offense

Student Offenders
These actions constitute offenses that shall or may result in placement in the Alternative Education Program located at F.S. Lara. The terms of a placement under this section shall prohibit the student from attending or participating in school-sponsored or school-related activities, including, but not limited to, extracurricular activities. A principal is not prohibited from suspending a student immediately prior to the student's placement in the Discipline Alternative Education Program (DAEP).

District Staff Offenders
Please contact the Human Resources Department to discuss consequences of violation. Generally, the district uses a progressive employee discipline system.

This involves giving the employee a verbal warning for a first offense and a written reprimand for the second. Third violations are treated on a case by case basis. However, if the violation is severe, the employee may be suspended and dismissed for cause without resorting to progressive discipline.

Reimbursement must be made for any costs that the district incurs due to the misuse or abuse of the system. Authorities may be notified at administrators' discretion. All possible legal actions will be taken against offenders. [See Policy DH]

Disclaimer of Liability

The District is not liable for inappropriate use of electronic communication resources, violations of copyright restrictions or other laws, mistakes or negligence, or costs incurred by

users. The District is not responsible for ensuring the accuracy, age appropriateness, or usability of any information found on the Internet.

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. (Local regulation CQ)

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.

STUDENT AGREEMENT FOR ACCEPTABLE USE OF THE ELECTRONIC COMMUNICATIONS SYSTEM

You are being given access to the District's electronic communications system. Through this system, you will be able to communicate with other schools, colleges, organizations, and people around the world through the Internet and other electronic information systems/networks. You will have access to hundreds of databases, libraries, and computer services all over the world.

With this educational opportunity comes responsibility. It is important that you read the District policy, administrative regulations, and agreement form and ask questions if you need help in understanding them. Inappropriate system use will result in the loss of the privilege to use this educational tool.

Please note that the Internet is a network of many types of communication and information networks. It is possible that you may run across areas of adult content and some material you (or your parents) might find objectionable. While the District will use filtering technology to restrict access to such material, it is not possible to absolutely prevent such access. It will be your responsibility to follow the rules for appropriate use.

RULES FOR APPROPRIATE USE

- You will be assigned an individual account, and you are responsible for not sharing the password for that account with others.
- The account is to be used mainly for identified educational purposes, but some limited personal use is permitted.
- You will be held responsible at all times for the proper use of your account, and the District may suspend or revoke your access if you violate the rules.
- Remember that people who receive e-mail from you with a school address might think your message represents the school's point of view.

INAPPROPRIATE USES

- Using the system for any illegal purpose.
- Disabling or attempting to disable any Internet filtering device.
- Encrypting communications to avoid security review.
- Borrowing someone's account without permission.
- Posting personal information about yourself or others (such as addresses and phone numbers).
- Downloading or using copyrighted information without permission from the copyright holder.
- Intentionally introducing a virus to the computer system.
- Posting messages or accessing materials that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.
- Wasting school resources through the improper use of the computer system.
- Gaining unauthorized access to restricted information or resources.
- Installing executable files that render a computer as a network device.

CONSEQUENCES FOR INAPPROPRIATE USE

- Suspension of access to the system;
- Revocation of the computer system account; or
- Other disciplinary or legal action, in accordance with the Student Code of Conduct and applicable laws.

The student agreement must be renewed each academic year.

AUP Guidelines

STUDENT AGREEMENT
FOR ACCEPTABLE USE OF THE
ELECTRONIC COMMUNICATIONS SYSTEM

Name _____ Grade _____

Student ID #: _____ School _____Year of Graduation: _____

You are being given access to the District's electronic communications system. Through this system, you will be able to communicate with other schools, colleges, organizations, and people around the world through the Internet and other electronic information systems/networks. You will have access to hundreds of databases, libraries, and computer services all over the world.

With this educational opportunity comes responsibility. It is important that you read the District policy, administrative regulations, and agreement form and ask questions if you need help in understanding them. Inappropriate system use will result in the loss of the privilege to use this educational tool.

Please note that the Internet is a network of many types of communication and information networks. It is possible that you may run across areas of adult content and some material you (or your parents) might find objectionable. While the District will use filtering technology to restrict access to such material, it is not possible to absolutely prevent such access. It will be your responsibility to follow the rules for appropriate use.

–*–*–*–*–

I have read the Electronic Communication and Data Management LISD guidelines and agree to abide by the provisions outlined. I understand that violation of these provisions may result in suspension or revocation of system access.

I also understand that the District has the right to and will monitor my any electronic activity on the computer system at any time (including computer usage, files, Internet usage, e-mail, and any distance learning activity). I understand that violation of these provisions may result in suspension or revocation of system access.

Student's signature _____ Date _____

PARENT OR GUARDIAN

I have read the Electronic Communication and Data Management LISD Guidelines. In consideration for the privilege of my child using the District's electronic communications system, and in consideration for having access to the public networks, I hereby release the District, its operators, and any institutions with which they are affiliated from any and all claims and damages of any nature arising from my child's use of, or inability to use, the system, including, without limitation, the type of damage identified in the District's policy and administrative regulations. I understand that the district will take necessary precautions to ensure the appropriate use of the electronic communications systems. I also understand it is not absolutely possible to prevent all improper use.

I am aware that my child's use of the District's communication equipment allows my child to participate in activities and lessons meeting the goals and objectives that are mandated by the State. I understand that my child will be involved with the following communication equipment and/or activities:

- Use of electronic technology equipment (including, but not limited to, computers, scanners, digital cameras, and video cameras)
- Use of the Internet and of distance learning activities (including, but not limited to, blogs, video conferencing, on-line conferences/instant messaging, and e-mail)
- Allow for their pictures to be taken for the use in any district's web page and electronic or printed presentations.
- Allow to have their work published on the Internet and Intranet (within the District)

☐ **Yes, I consent to have my child involved with all of the above communication equipment.**

☐ No, I do not consent to have my child involved with all of the above communication equipment. I will include a note with this form explaining what I do not consent to.

Signature of parent or guardian _____

NONSCHOOL USER AGREEMENT
FOR ACCEPTABLE USE OF THE ELECTRONIC COMMUNICATIONS SYSTEM

Check one:

☐	Parent of a student at this campus	☐	Visitor (not from this neighborhood)
☐	Community member	☐	School Board Member
☐	Vendors, Subcontractors		

User Name: (Please Print) _____

Date _____ Home phone number _____

Which neighborhood campus will you most likely be using for the use of computers and/or system access? _____

You are being given access to the District's electronic communications system. Through this system, you will be able to communicate with other schools, colleges, organizations, and people around the world through the Internet and other electronic information systems/networks. You will have access to hundreds of databases, libraries, and computer services all over the world.

With this educational opportunity comes responsibility. It is important that you read the District policy, administrative regulations, and agreement form and ask questions if you need help in understanding them. Inappropriate system use will result in the loss of the privilege to use this educational tool.

Please note that the Internet is a network of many types of communication and information networks. It is possible that you may run across areas of adult content and some material you (or your parents) might find objectionable. While the District will use filtering technology to restrict access to such material, it is not possible to absolutely prevent such access. It will be your responsibility to follow the rules for appropriate use.

I have read the Electronic Communications and Data Management LISD Guidelines and agree to abide by their provisions. In consideration for the privilege of using the District's electronic communications system and in consideration for having access to the public networks, I hereby release the District, its operators, and any institutions with which they are affiliated from any and all claims and damages of any nature arising from my use of, or inability to use, the system, including, without limitation, the type of damages identified in the guidelines.

Signature _____

EMPLOYEE AGREEMENT FOR ACCEPTABLE USE OF THE ELECTRONIC COMMUNICATIONS SYSTEM

You are being given access to the District's electronic communications system. Through this system, you will be able to communicate with other schools, colleges, organizations, and people around the world through the Internet and other electronic information systems/networks. You will have access to hundreds of databases, libraries, and computer services all over the world.

With this opportunity comes responsibility. It is important that you read the District policy, administrative regulations, and agreement form and ask questions if you need help in understanding them. Inappropriate system use will result in the loss of the privilege of using this educational and administrative tool.

Please note that the Internet is a network of many types of communication and information networks. It is possible that you may run across some material you might find objectionable. While the District will use filtering technology to restrict access to such material, it is not possible to absolutely prevent such access. It will be your responsibility to follow the rules for appropriate use.

RULES FOR APPROPRIATE USE

- **The account is to be used mainly for educational purposes, but some limited personal use is permitted.**
- **You will be held responsible at all times for the proper use of your account, and the District may suspend or revoke your access if you violate the rules.**
- **Remember that people who receive e-mail from you with a school address might think your message represents the school's point of view.**

INAPPROPRIATE USES

- **Using the system for any illegal purpose.**
- **Disabling or attempting to disable any Internet filtering device.**
- **Encrypting communications to avoid security review.**
- **Borrowing someone's account without permission.**
- **Downloading or using copyrighted information without permission from the copyright holder.**
- **Intentionally introducing a virus to the computer system.**
- **Posting messages or accessing materials that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal.**
- **Wasting school resources through improper use of the computer system.**
- **Gaining unauthorized access to restricted information or resources.**
- **Falsifying or not reporting correct data.**

CONSEQUENCES FOR INAPPROPRIATE USE

- **Suspension of access to the system;**
- **Revocation of the computer system account; or**
- **Other disciplinary or legal action, in accordance with the District policies and applicable laws.**

I understand that my computer use is not private and that the District will monitor my activity on the computer system.

Updated: August 2010

EMPLOYEE AGREEMENT

FOR ACCEPTABLE USE OF THE ELECTRONIC COMMUNICATIONS SYSTEM

Date: _____ **Employee ID#** _____

Employee Name: (Please Print): _____

Campus/Dept.: _____ **Campus/Dept. Phone#:** _____

PLEASE INITIAL OR WRITE N/A IF NOT APPLICABLE (Do not leave any blanks):

_____**I have read the District's Electronic Communication and Data Management LISD Guidelines and agree to abide by their provisions. I understand that violation of these provisions may result in suspension or revocation of system access and possible disciplinary action. In consideration for the privilege of using the District's electronic communication system and in consideration for having access to the public networks, I hereby release the District, its operators, and any institutions with which they are affiliated from any and all claims and damages of any nature arising from my use of, or inability to use, the system, including, without limitation, the type of damages identified in the District's policy and administrative regulations.**

_____**I understand that my use of the LISD's technology equipment is not private and that the District will do electronic auditing, monitoring within all unclassified networks that connect to the Internet or other publicly accessible networks to support identification, termination and protection of any unauthorized activity.**

_____**I hereby certify the information provided above is correct and complete. I certify that the requesting party will follow the FERPA statue, 20 U.S.C. § 1232g, regulations, 34 C.F.R. Part 99, and other applicable law. I certify that the requested information will be used for the stated purpose(s) and the data will be kept under a secured/password secured environment. And I certify that if an unauthorized person has had access to this file, I will contact PEIMS Coordinator as soon as possible and report it.**

_____**I will not falsify any information.**

_____**I understand that my computer and files are the property of LISD and that the District has the right to or delete any unapproved software and will monitor my activity on the student information system at any time.**

_____**As an employee and/or educator of the Laredo Independent School District, I will have access to the user names and passwords of students and the District. Therefore, it is my responsibility to ensure that there is no misuse of this highly confidential information. It is also my duty and responsibility to report any witnessed misuse of student or district information.**

_____ _____

Signature **Date**

_____**e-mail Address**

Updated: August 2010

Credits

Some of the ideas and/or information were obtained from the following sources:
Texas Association of School Boards (TASB) Policy and Regulations on Electronic Communication and Data Management.

The Center for Distance Learning Research—Texas A&M University. "Videoconferencing: A Basic Guide to Teaching Using Videoconferencing Equipment", p.4

References below are for Developing and Publishing of Web Pages:

http://www.kckps.k12.ks.us/techplan/interstu.html

July 2010 LISD's Instructional Technology Department accepted the challenge of revising the Acceptable Use Policies.

The revision of the guidelines is a collaborative effort by the following:
Elizabeth Jo Garcia, Director for Instructional Technology
Miguel Munoa, Chief Technology Officer
Ambrosio Gomez, Information Security Analyst
Guillermo Villarreal, Technology Coordinator
Norma Villarreal, District Technology Trainer
Arabella Castillo, District Technology Trainer
Noemi Vidaurri, Software Specialist/Trainer
Lead Technicians: Hilario Solis, Joe Estrada,
And input from Technology Trainers and the Technology Task Force Committee members