LAREDO INDEPENDENT SCHOOL DISTRICT
TECHNOLOGY
SERVICES DEPARTMENT

Acceptable Use Policies and Guidelines

Revised: July 2018

Table of Contents

Laredo Independent School District
Board of Trustees

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

It is the policy of the Laredo Independent School District not to discriminate on the basis of race, color, national origin gender, limited English proficiency, or handicapping condition in its programs.

Technology Educational Goals

(Technology Plan, 2018 - 2019)

- **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 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 Services 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 will strive to have quality, updated school and department websites in order to provide effective information to staff, students, parents and community.
  - **Objective 3.2:** LISD will establish a teacher recognition program that emphasizes and rewards teachers for their exemplary use of technology in the classroom.
  - **Objective 3.3:** LISD staff will identify budget and secure funding to support technology identified in all classroom, libraries, campus and district planning efforts.
  - **Objective 3.**4: 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 (E-rate) 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 Services 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 are intended to make the district's technology equipment and networking/communication tools, which will be referred to as technology resources, more efficient, accessible, and reliable for all users.

"User" is defined as anyone with access to LISD's technology equipment and networking/communications tools.

Some examples of technology equipment include laptops, desktop computers, printers, projectors, iPads, servers, Wi-Fi access points, and digital signage monitors. This is not an exhaustive list of items that can be classified as technology equipment.

Some examples of "Networking/Communications Tools" include: approved social media, webpages, district apps, distance learning, blogs and electronic mail.

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 these resources. Use of these resources is primarily for instructional and administrative purposes and in accordance with administrative regulations.

The use of the district's technology equipment and/or networking/communication tools is a privilege and not a right.

Bring Your Own Devices (BYODs)

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. For the purpose of these guidelines, these devices will be referred to as "Bring Your Own Devices" (BYODs). BYODs using or accessing district resources (i.e. Wi-Fi) 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 BYODs. Maintenance and troubleshooting of BYODs is solely the responsibility of the student or employee possessing the device. The district is not responsible for loss, theft and/or damages to BYODs 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 or via electronic signature (UETA 2001) 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 Employee Handbook.)

Digital Citizenship

International Society for Technology in Education (ISTE) Standard 3 for Educators states: Educators inspire students to positively contribute to and responsibly participate in the digital world.
ISTE Standard 2 for Students states: Students recognize the rights, responsibilities and opportunities of living, learning and working in an interconnected digital world, and they act and model in ways that are safe, legal and ethical.

The two standards mentioned above serve as the foundation for the creation of these Acceptable Use Policies (AUP).

All Laredo Independent School District's technology resources is to be used for instructional and administrative purposes. These purposes include any activities that support the district's instructional goals and objectives. Limited personal use of the system shall be permitted if the use: 1) imposes no noticeable cost on the district; 2) does not burden the district's technology resources; and 3) has no negative effect on the performance of the employee or student.

Educators/Employees must not use any networking/communication tools to send text messages to students unless conducted via safe group texting sites approved by the district such as Remind or Class Dojo.

Acceptable and Unacceptable Uses of the District's Technology Resources

Any user of the district's resources is required to use them in an ethical and legal manner. Below is a list of some the most common acceptable and unacceptable uses of district resources. This list is not exhaustive and any suspected violations will be treated on a case-by-case basis. In addition, any user who sees another user violating the AUP has the duty to report that user to an administrator at the campus or department.

Examples of Acceptable Uses

- Users shall protect the security and privacy of LISD's technology resources.
- Users shall use technology resources in an ethical, legal, and safe manner.
- 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).
- Users of district-issued technology equipment should immediately report any damage, theft, or misplacement of this equipment to the Technology Services Department.
- Users shall use the Internet for educational and administrative purposes and as a tool to enhance teaching and learning in the classroom.
- All passwords must remain confidential and should not be shared. In sites where the user creates a password. It shall be a strong eight-character password that contains at least

one uppercase letter, one lowercase letter, and one number. It should not include your username, email, employee/student ID or first/last name. *(Local regulation CQ)*

- 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)*
- Users shall demonstrate respect for the rights and obligations of using and sharing intellectual property. *(ISTE Student Standard 2c, Educator Standard 3c)*
- 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)*
- Users shall conserve district resources (paper in printer, disk space, bandwidth, etc.).
- Users are expected to observe the following network etiquette: *(Local regulation CQ) (ISTE Student Standard 2b, Educator Standard 3a)*
  - Be polite; messages typed in capital letters are the computer equivalent of shouting and are considered rude.
  - Not engage in communication that may be considered cyberbullying, trolling, or scamming.
  - Use appropriate language. Swearing, vulgarity, ethnic or racial slurs and any other inflammatory language are prohibited.
  - Not pretend to be someone else when sending/receiving messages when using district resources.
  - Not engage in social engineering practices in attempts to obtain access to another person's personal information or gain access to restricted systems.
- Users shall be observant that the use of the district's networking/communication tools might cause some recipients to assume they represent the district or school, whether or not that was the user's intention.

Unacceptable Uses

- Users shall not hack or otherwise alter programs or files belonging to other users.
- Users shall not take actions that are harmful to any of the district's technology equipment. (vandalism)
- Users shall not remove any district technology equipment from US boundaries.
- Users shall not use the computer/technology equipment in any way that may harass, defame or demean others with language, image or threats.
- Users shall not use district technology resources for personal use such as for commercial purposes, financial gain, advertisement, and seeking/interacting with professional unions, political lobbying, and supporting illegal activities. *(Local Regulation CQ)*
- Users shall not use/download any non-educational sites, social media sites, and file sharing sites or resources unless approved by the district.
- Users shall not make any changes to the computer/technology equipment configurations (i.e. network settings).
- Users shall not use unauthorized administrative logins and passwords without the written approval from the Director of Instructional Technology or Assistant Superintendent for Technology Services.

- 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 district technology resource. Such software is often called a bug, virus, worm, Trojan horse, or similar name.
- Users shall not assemble or disassemble computers/technology equipment without written permission from Director of Instructional Technology or Assistant Superintendent for Technology Services.
- 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.)
- Users may not disable, or attempt to disable, a filtering device on the district's technology equipment. *(Local regulation CQ)*
- Users shall not encrypt communications so as to avoid security review by system administrators. *(Local regulation CQ)*
- Users shall not use student/staff system account without written permission from the campus administrator or Technology Services Department. *(Local regulation CQ)*
- 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 may not use the district's technology resources to gain unauthorized access to resources or information. *(Local regulation CQ)*
- Users shall not distribute personal information about themselves or others while using district technology resources. (Local regulation CQ)
- Users shall not purposefully access, post, or send to other users, 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:
    - Sites with images or text that is provocative, suggestive and/or erotic in nature.
    - Sites that promote activities which are illegal for minors (such as drinking alcohol)
    - Sites that contain content a "reasonable person" may find repulsive or disgusting.
    - Sites that promote criminal activity. Examples include, but not limited to:
        - Building bombs or explosives
        - Hacking into computer systems
        - Lock picking
        - Sites that promote the use of illegal controlled substances or instruct the reader how to grow/make/process these substances.
        - Sites that allow the playing or downloading non-educational games.
        - Sites that allow on-line gambling or are dedicated to gambling information and instructions.

    - Sites that advocate intolerance or hatred of a person or group of people (gangs).
    - Sites that show or advocate violence. Examples include: Images containing graphic violence (blood/murder), promotion of violence or terrorist acts against others.

- ➢ 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 networking/communication 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.
- ➢ Users shall not share their login or password with anyone. *(Local regulation CQ)*
- ➢ 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)*
- ➢ 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.
- ➢ Users shall not try to gain entry into another user's computer or other technology equipment.
- ➢ Users shall not try to gain entry into another user's networking/communications account.
- ➢ Users shall not identify students on school's web pages unless permission was granted by the parent or legal guardian.

    Users shall follow these guidelines:

    - ▪ 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.
    - ▪ Student work shall not reveal family or personal details that may be construed as invasion of privacy for student or family members.
    - ▪ Student pictures shall not be published unless written parental permission or student (for students over 18 years of age) permission is obtained.

Social Engineering

The purpose of social engineering is to secretly install spyware or other malicious software to trick an individual into handing over passwords, personal information, or other sensitive financial data.

Note: The Technology Services Department will NEVER ask for a user's password over email. Users must exercise caution when encountering emails asking for personal information. Users must not open and such emails or download any files from these types of emails.

Users have a responsibility to immediately REPORT any suspicious emails to the Technology Services Department.

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, Instruction, and Assessment Department for content then by the Technology Services 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 Technology Services Department or designee will perform installation.
- Software may not be purchased solely for individual use unless approved by the Curriculum, Instruction, and Assessment Department. (Exception: iPad apps after approval for purchase by District Technology Services 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. Assistant Superintendent for Technology Services must approve all such technology equipment and software before purchase is made.

Local DH Code of Ethics and Standard Practice for Texas Educators, Regulations. Violations of law may result in criminal prosecution 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 resources, BYODs 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:

- Filtering will be provided for all Internet enabled computers used by students, patrons, and staff.
- Requiring BYODs to log onto the district's network when accessing or using district resources to enable filtering.
- Filtering will be disabled only for bona fide research or other lawful purposes.
- Online activities of minors will be monitored for appropriate use.
- Safe and secure use by minors of direct electronic communications will be assured.
- 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.

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 Acceptable Use Policy when using district technology resources or when participating in a school-related activity.

Any violations of the AUP will be looked at on a case-by-case basis to determine the level of the violation. Violations can be classified as Level I, II, and III. Once a level of violation is decided, the disciplinary actions will be aligned with those denoted in the Student Code of Conduct for the district.

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 Policy 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 administrator 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

If a violation of the AUP is classified as Level I, the following consequences may occur.

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 district technology resources 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 resources, or the equipment or data of any of the agencies or other networks that are connected to our network.
- 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 or post messages, or use hand gestures that are abusive, obscene, sexually oriented, threatening, harassing, or damaging to another's reputation while using distance learning apps or programs.
- 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]

<u>Level III Violation/ Offense</u>

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 district's technology 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 technology resources.

Student Agreement for Acceptable Use of Technology Resources

You are being given access to the district's technology resources. Through this resource, you will be able to communicate with other schools, colleges, organizations, and people around the world through the Internet and other networking/communication sites. 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 not to share the password for your 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 technology resources 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.

STUDENT AGREEMENT
FOR ACCEPTABLE USE OF DISTRICT TECHNOLOGY RESOURCES

Name ____ Grade ____________________

Student ID #: ______________ School __________________Year of Graduation: _____

You are being given access to the district's technology resources. 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 Acceptable Use Policies 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 District’s Acceptable Use Policy. In consideration for the privilege of my child using the district's technology resources, 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 technology resources 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, distance learning, approved social media sites, approved messaging apps, 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 DISTRICT TECHNOLOGY RESOURCES

Check one:

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

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 technology resources. Through this resource, 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 District’s Acceptable Use Policy and agree to abide by their provisions. In consideration for the privilege of using the district's technology resources 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 DISTRICT TECHNOLOGY RESOURCES

You are being given access to the district's technology resources. Through this resource, 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 use will result in the loss of the privilege of using the district's technology resources.

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.

EMPLOYEE AGREEMENT

FOR ACCEPTABLE USE OF DISTRICT TECHNOLOGY RESOURCES

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 Acceptable Use Policies 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 technology resources 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 resources 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

Credits

Some of the information included in these policies and guidelines was 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

The revisions included in these policies and guidelines were completed by LISD's Technology Services Department.

Miguel Munoa, Assistant Superintendent for Technology Services

Brenda Sepulveda, Director of Instructional Technology

Guillermo Villarreal, Instructional Technology High School Coordinator

Jorge Muñoz, Instructional Technology Middle/Specialty School Coordinator

Arabella Castillo, Instructional Technology District Specialist/Trainer