Electronic Acceptable Use Policies

2017-2018
Online AUP Training

LAREDO INDEPENDENT SCHOOL DISTRICT
TECHNOLOGY

Training Goal

The purpose of this training is to:

- Review LISD's Electronic Acceptable Use Policies (AUP) which set forth the district's acceptable use of electronic systems.
- The Electronic Acceptable Use Policies (AUP) are intended to make the district's technology equipment, applications/programs and the system network more efficient, accessible and reliable for all users.
- It is our goal to instruct all employees concerning the ethical, legal and safe use of:
  - Technology Equipment: e.g. computers, laptops, mobile devices, printers, scanners, distance learning equipment and other electronic equipment as described in the policies.
  - Network: e.g. Internet, e-mail, approved social media sites (i.e. Edmodo), discussion groups, blogs, distance learning, etc.

We will also review some of limitations as prescribed in LISD's CQ administrative regulation.

Who is the *USER*?

Anyone with access to LISD's network, computer equipment or programs.

Laredo ISD……

- students
- employees
- volunteers
- community members

Guests…

- vendors
- consultants
- service providers
- employees of subcontracted companies

Use of the LISD network and any district-owned equipment will primarily be used for instructional or administrative purposes.

- Instructional purposes can be defined as any activity or usage that aligns with the district's instructional goals and objectives.
- Administrative purposes can be defined as any usage that allows the employee to effectively fulfill their job requirements.
- Limited personal use of the system shall be permitted if the use: 1) imposes no tangible cost to 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.

LISD Expectations

All LISD employees who use technology will…

- review and understand this training
- register on Eduphoria before or after this training
- take a quiz after this training
- pass the quiz
- sign an electronic agreement form on an annual basis to continue using LISD's network.
- continue to use technology in an ethical, legal and safe way

It is a *privilege* and not a *right* to…

- Use the district's technology equipment
- Participate in any online communication service such as, but not limited to:
  - Internet and e-mail
  - ALIO
  - Workflow
  - DMAC
  - Distance Learning (Video Conference)
  - Web Pages
  - Student Information System
  - Skyward (Gradebook & Attendance System)

Password Policy

- **General Password Construction Guidelines**

  All users at Laredo Independent School District should be aware of how to select strong passwords.

Strong passwords have the following characteristics:

- **Contain at least the following character classes:**
  - one lower case character
  - one upper case character
  - one number
- **May not contain your username, email, first name, employee ID or last name**
- **Password must not contain spaces**
- **Contain at least eight alphanumeric characters.**
- **Password must be changed every 60 days**.

Weak passwords have the following characteristics:

- The password contains less than eight characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
  - Names of family, pets, friends, co-workers, fantasy characters, etc.
  - Computer terms and names, commands, sites, companies, hardware, software.
  - The words "Laredo Independent School District", "laredo", "laredoisd" or any derivation.
  - Birthdays and other personal information such as addresses and phone numbers.
  - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
  - Any of the above spelled backwards.
  - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Personal Telecommunications/Electronic Devices (PTEDs)

- PTEDs defined: devices include but are not limited to smart phones, laptops, tablets, electronic readers (Nook, Kindle) netbooks, etc.
- Employees and Students are allowed to use PTEDs (also known as BYOD: Bring Your Own Device) on LISD's network but its use must still adhere to LISD's Acceptable Use Policies (AUP).
- The Technology Services Department does not address any technical issues related to PTEDs. Maintenance or troubleshooting of PTEDs is the sole responsibility of the student or employee possessing the device.

Use of Electronic Media with Students

The employee may use any form of electronic media except text messaging. Only a teacher, trainer, or other employee who has an extracurricular duty may use text messaging and only to communicate with students who participate in the extracurricular activity over which the employee has responsibility.

Prohibited texting with students does not include safe group texting sites, such as *Remind*. Administrators, instructional teachers, and counselors who do not have an extracurricular duty may use *Remind* to communicate with students through text messaging.

LISD Acceptable Use Policy

The next slides will go over some of the practices not allowed while using any part of LISD's technology equipment, network, resources or programs owned by the district.

This is not an exhaustive list and only highlights some of the most common misuses. To get a full and up-to-date version of the Acceptable Use Policy and Employee Handbook, please visit our district website.

LISD Acceptable Use Policy (cont.)

Users of LISD's network, equipment and programs must **not** do the following:

- Attempt to hack network resources or resources of other users.
- Share usernames and password or use someone else's username and password.
- Take actions that can result in harming or disrupting the functionality or performance of the district's network or resources.
- Use computer/technology equipment in any way that may harass, defame, or demean others with language, image or threats.
- Remove any district technology equipment from US boundaries.

Equipment cannot go into Mexico, this includes district laptops!

(Due to Microsoft products being subject to export restrictions under U.S. law because they include encryption technology, and the district's equipment insurance coverage, LISD does not permit their equipment to leave the United States.)

LISD Acceptable Use Policy (cont.)

Users of LISD's network, equipment and programs must **not** do the following:

- Use unauthorized administrative logins and passwords.
- Perform any actions that infringe on any copyright laws.
- Misuse district resources (i.e. printers, paper, invitations, etc.) for personal use.
- Assemble or disassemble computer/technology equipment.
- Move computer/technology equipment from designated areas without getting administrator approval to do so and then originating the district approved fixed assets transfer process.
- Act, or fail to act, in use of software, in a manner that is contrary to applicable law or regulation.

LISD Acceptable Use Policy (cont.)

Users of LISD's network, equipment and programs must **not** do the following:

- Transfer any images that can deemed as offensive or vulgar.
- Use the network for promoting political agendas.
- Use the network to send chain letters, messages, images or files that can be considered spam as these are considered not instructional in nature.
- Fail to report the observed misuse of another user to their appropriate administrator or supervisor.
- Mimic another district user's identity.

LISD Acceptable Use Policy (cont.)

As an employee, you may need to access confidential student information/educational records for planning instruction, attendance, and grades. At times, you may also need to access confidential personnel information.

Under federal guidelines through **Family Educational Rights and Privacy Act** (FERPA), you are legally and ethically obligated to safeguard the confidentiality of any information records may contain.

District Software Usage

Software Purchases/Installation/Usage

All software purchases or acquisitions must follow outlined district guidelines or may result in the district exercising its right to remove any unauthorized software from district technology.

All instructional software must first be approved by the **Curriculum and Instruction** Department for content, then by the **Technology Services** Department for compatibility with hardware and/or network. *(procedure subject to change)*

Student Training

LISD is providing access to the internet and certain district resources to students with the purpose to facilitate teaching and learning of the curriculum in accordance with Laredo ISD educational objectives. Before a student can be granted access, the teacher must do the following.

- Student Internet Safety Training by the homeroom teacher.
- A Student Agreement Form signed by the parent.
- Student verification/activation of account via Skyward/Student Activation link.

Teachers are responsible to make sure students are using the district's network and resources in a manner that is aligned with their educational goals.

LISD Filtering System

Although LISD's filtering system is compliant with the Children's Internet Protection Act of 2001 (CIPA), there still may be instances where users unintentionally encounter inappropriate material. Some examples of inappropriate material include:

- Adult Sites
- Crime Sites
- Gambling Sites
- Violence Sites

If a user does encounter such material, they must immediately discontinue access and refer this information to administrator, supervisor, or campus technology trainer.

Phishing

- **What is Phishing?**
  - Phishing email messages, websites, and phone calls are designed to steal money or sensitive information. Cybercriminals can do this by installing malicious software on your computer, tricking you into giving them sensitive information, or outright stealing personal information off of your computer.

- **Types of Phishing Attacks**
  - Social Engineering - On your Facebook profile or LinkedIn profile, you can find: Name, Date of Birth, Location, Workplace, Interests, Hobbies, Skills, your Relationship Status, Telephone Number, Email Address and Favorite Food. This is everything a Cybercriminal needs in order to fool you into thinking that the message or email is legitimate.
  - Link Manipulation - Most methods of phishing use some form of deception designed to make a link in an email appear to belong to the spoofed organization or person. Misspelled URLs or the use of subdomains are common tricks used by phishers. Many email clients or web browsers will show previews of where a link will take the user in the bottom left of the screen or while hovering the mouse cursor over a link.
  - Spear phishing - Phishing attempts directed at specific individuals or companies have been termed spear phishing. Attackers may gather personal information (social engineering) about their targets to increase their probability of success. This technique is, by far, the most successful on the internet today, accounting for 91% of attacks.
  - Clone phishing - A type of phishing attack whereby a legitimate, and previously delivered email containing an attachment or link has had its content and recipient address(es) taken and used to create an almost identical or cloned email. The attachment or link within the email is replaced with a malicious version and then sent from an email address spoofed to appear to come from the original sender.

Phishing (cont.)

- **Tips to protect yourself from Phishing emails.**
  - I.T. will NEVER ask for your password over email. Please be wary of any emails asking for passwords. Never send passwords, bank account numbers, or other private information in an email.
  - Be cautious about opening attachments and downloading files from emails, regardless of who sent them. These files can contain viruses or other malware that can weaken your computer's security. If you are not expecting an email with an attachment from someone, such as a fax or a PDF, please call and ask them if they indeed sent the email.
  - Look for 'https://' and a lock icon in the address bar before entering any private information on a website.
  - Look for spelling and bad grammar. Cybercriminals are not known for their grammar and spelling. Professional companies or organizations usually have staff that will not allow a mass email like this to go out to its users. If you notice mistakes in an email, it might be a scam.

- **What to do when you think you received a phishing email.**
  - First, do not click on any links within the email or download any attachment. Forward the email to abuse@laredoisd.org for Information Security to examine and determine if legitimate.
  - If there is an attachment in the email, and you recognize the sender but aren't expecting an attachment from them, please call them and ask if it is legitimate.

Social Engineering

What is Social Engineering?

- It is manipulating a person into knowingly or unknowingly giving up information; essentially 'hacking' into a person to steal valuable information.
- It is a way for criminals to gain access to information systems. The purpose of social engineering is usually to secretly install spyware, other malicious software or to trick persons into handing over passwords and/or other sensitive financial or personal information.
- Social engineering is one of the most effective routes to stealing confidential data from organizations.

Popular types of social engineering attacks include:

- Baiting: Baiting is when an attacker leaves a malware-infected physical device, such as a USB flash drive in a place it is sure to be found. The finder then picks up the device and loads it onto his or her computer, unintentionally installing the malware.
- Phishing: Phishing is when a malicious party sends a fraudulent email disguised as a legitimate email, often purporting to be from a trusted source. The message is meant to trick the recipient into sharing personal or financial information or clicking on a link that installs malware.
- Spear phishing: Spear phishing is like phishing, but tailored for a specific individual or organization.
- Pretexting: Pretexting is when one party lies to another to gain access to privileged data. For example, a pretexting scam could involve an attacker who pretends to need personal or financial data in order to confirm the identity of the recipient.
- Scareware: Scareware involves tricking the victim into thinking his computer is infected with malware or has inadvertently downloaded illegal content. The attacker then offers the victim a solution that will fix the bogus problem; in reality, the victim is simply tricked into downloading and installing the attacker's malware.

Social Engineering (cont.)

Don’t become a victim

- Slow down. Spammers want you to act first and think later. If the message conveys a sense of urgency, or uses high-pressure sales tactics be skeptical; never let their urgency influence your careful review.
- Research the facts. Be suspicious of any unsolicited messages. If the email looks like it is from a company you use, do your own research. Use a search engine to go to the real company’s site, or a phone directory to find their phone number.
- Delete any request for financial information or passwords. If you get asked to reply to a message with personal information, it’s a scam.
- Reject requests for help or offers of help. Legitimate companies and organizations do not contact you to provide help. If you did not specifically request assistance from the sender, consider any offer to ’help’ restore credit scores, refinance a home, answer your question, etc., a scam. Similarly, if you receive a request for help from a charity or organization that you do not have a relationship with, delete it. To give, seek out reputable charitable organizations on your own to avoid falling for a scam.
- Don’t let a link in control of where you land. Stay in control by finding the website yourself using a search engine to be sure you land where you intend to land. Hovering over links in email will show the actual URL at the bottom, but a good fake can still steer you wrong.

Audits and Monitoring

User must understand that…

- LISD ***will*** periodically audit, inspect, and/or monitor ***all*** use of LISD's technology - inclusive of remote and/or online resources, email, and storage media as deemed appropriate.

- LISD ***will*** take disciplinary action if ***any*** violations of district policies and regulations are found.

Disciplinary Action

- Students and staff must follow all District's Acceptable Use Policy (AUP) and Guidelines 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.

Disclaimer of Liability

The District will cooperate fully with local, state, or federal law enforcement agencies in any investigation concerning or relating to misuse of the District's equipment and/or District's electronic communication system.

NOTE:
These guidelines are updated yearly.
Adoption of additional policies or revisions may occur any time during the school year.

It is your responsibility to...

- Review all of the AUP Guidelines found on LISD's website.
- Report any improper use of computer/Internet to your administrator and/or Director of Instructional Technology, Elizabeth J. Sandoval at 273-1340 or email to ejsandoval@laredoisd.org
- Report any missing or modified files from your computer to the IT Department at 273-1330.

Register on Eduphoria

- If you have not registered on Eduphoria, register now:
- Go to the following site:

  LISD homepage: http://www.laredoisd.org> For Employees > eSystems >Eduphoria>Workshop>eCourse
- Find the training session by searching for: ***2017-2018 Acceptable Use Policies.***

Now, you need to take the quiz…

Any questions regarding this training please contact your campus technology trainer.

District and Central Office staff may contact the Instructional Technology Department at 273-1340.