Technology Acceptable Use Policies (AUP) for District Users

Online Training

LISD LAREDO

Learning Objectives

- Understand the purpose of district **technology resources**.
- Identify who is considered a district **technology user**.
- Comprehend the district **expectations** when utilizing technology resources.
- Distinguish examples of **unacceptable uses** of technology resources.
- Recognize the importance of **FERPA, Cybersecurity Training, LISD's Filtering System, BYODs, and Student Training Requirements.**
- Be aware of the process of **audits, disciplinary actions, and the district's disclaimer of liability**.

LAREDO INDEPENDENT SCHOOL DISTRICT
TECHNOLOGY
SERVICES DEPARTMENT

Purpose of Technology

District users are provided technology resources *primarily* for both INSTRUCTIONAL and ADMINISTRATIVE purposes.

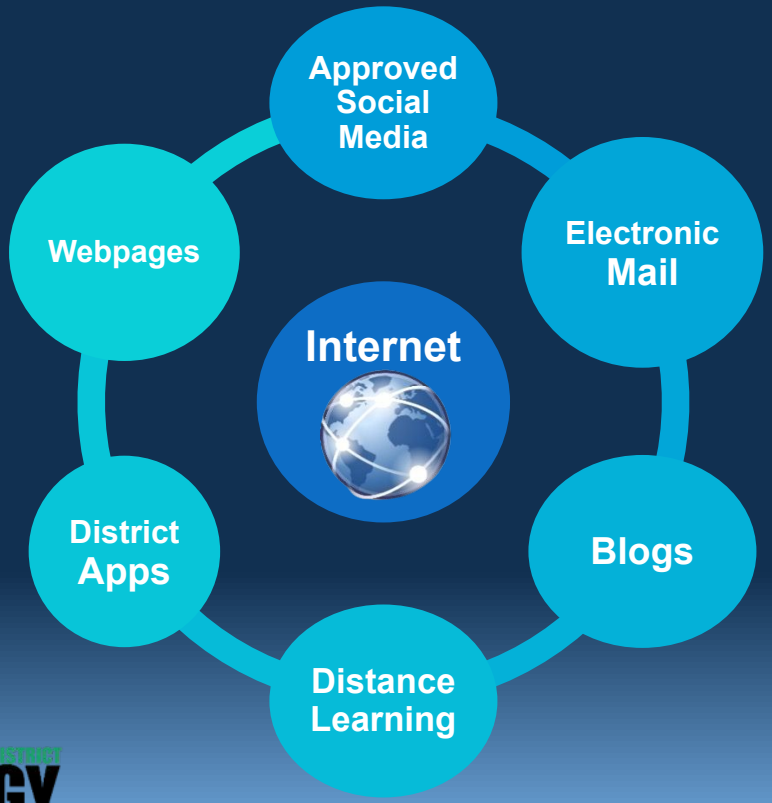
District users are responsible for understanding the ethical, legal, and safe use of both technology equipment and networking/communication tools.

LAREDO INDEPENDENT SCHOOL DISTRICT
TECHNOLOGY
SERVICES DEPARTMENT

Examples of:

Technology Equipment

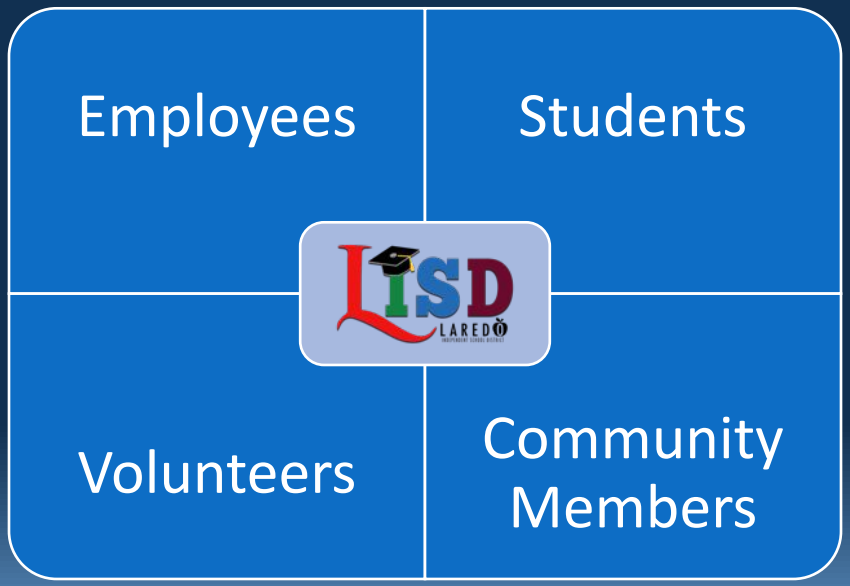
Networking/ Communication Tools

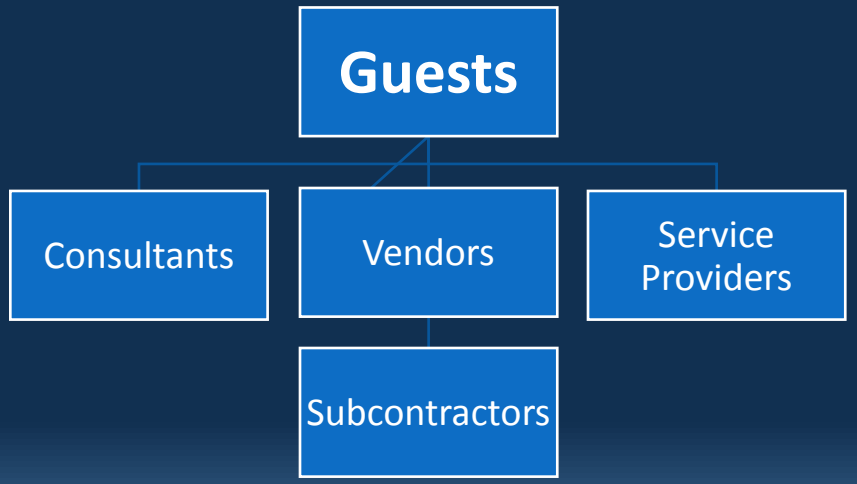


LAREDO INDEPENDENT SCHOOL DISTRICT
TECHNOLOGY
SERVICES DEPARTMENT

Who is considered a technology user?

Anyone with access to LISD's technology equipment and networking/communication tools is considered a user.





LAREDO INDEPENDENT SCHOOL DISTRICT
TECHNOLOGY
SERVICES DEPARTMENT

The use of technology is a privilege, not a right.

Users will be held responsible at all times to ensure that the proper use of technology:

- aligns with the district's goals and objectives.
- fulfills their job requirements.

Limited personal use is permitted when it:

1.) imposes no noticeable cost to 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.

LAREDO INDEPENDENT SCHOOL DISTRICT
TECHNOLOGY
SERVICES DEPARTMENT

User Expectations

- ✔ Read and understand the acceptable uses for technology resources.
- ✔ Register for AUP training and successfully pass the quiz.
- ✔ Digitally sign electronic agreement form on an **annual** basis to continue to use district technology resources.
- ✔ Create a **strong** ten-character password that contains at least one uppercase letter, one lowercase letter, one number, and one special character. It should **not** include your username, email, employee ID, or first/last name.
- ✔ Use technology resources in an ethical, legal, and safe manner.

***This is a condensed version of the district's AUP. To get the full, up-to-date version of the Acceptable Use Policy and Employee Handbook, please visit the district website HERE.**

Unacceptable Uses

The following are some examples of unacceptable uses of the district's technology resources.

Logging On

- Attempting to log on or actually logging into a computer or email account as **another user**.
- Attempting to hack network resources or resources of others.
- Take actions that can result in harming or disrupting the functionality of the district's network or resources.

Passwords

- Using administrative logins or passwords not assigned to you.
- Sharing usernames and passwords with someone else.
- Mimic another user's identity.

Equipment

- Using equipment in any way that may harass, defame, or demean others through language, images or threats.
- Removal of any equipment from designated areas without approval or removing from **US boundaries**.
- Misuse of equipment for personal reasons (such as printers, paper, etc.)
- Assemble or disassemble equipment.

LAREDO INDEPENDENT SCHOOL DISTRICT
TECHNOLOGY
SERVICES DEPARTMENT

Unacceptable Uses

The following are some examples of unacceptable uses of the district's technology resources.

Software

- Act, or fail to act, in a matter that is contrary to applicable law or regulation when using software.
- Purchase or acquire software **without the consent** of the Curriculum, Instruction, and Assessment **and** Instructional Technology Departments. **Form to be filled prior to purchase.**

Electronic Mail

- Use of the network for promoting political agendas.
- Use of the network to send chain letters, messages, images, or files that can be considered spam.
- Transfer any images that can be deemed offensive or vulgar.

Electronic Media

- Inappropriate text messages to students that are not conducted through safe group texting sites, such as Remind or Class Dojo.
- Failure to report the observed misuse of another user to their appropriate administrator or supervisor.

LAREDO INDEPENDENT SCHOOL DISTRICT
TECHNOLOGY
SERVICES DEPARTMENT

Family Educational Rights and Privacy Act (FERPA)

Under federal guidelines through FERPA, employees are legally and ethically obligated to safeguard the confidentiality of any information records may contain.

LAREDO INDEPENDENT SCHOOL DISTRICT
TECHNOLOGY
SERVICES DEPARTMENT

User Expectations for Virtual Meetings – All Users

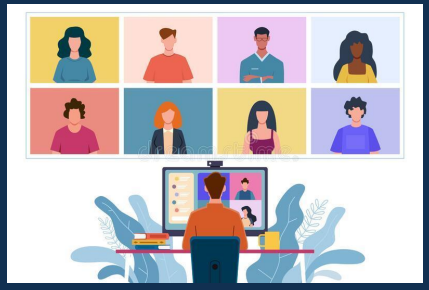
- **Host** a virtual meeting using district-approved systems, such as Google Meet, WebEx, or Skype. Users may **join** a virtual meeting using other systems as long as they use due diligence and an updated web browser to connect. Downloading virtual conferencing systems that are **not** district-approved may put you or the district at risk.
- Be on time. Log in a few minutes prior to the meeting to ensure connectivity.
- Find a place to conduct the virtual meeting with few distractions. Be aware of your background. No inappropriate materials should be visible.
- Turn on your camera and mute your microphone upon entering the meeting. Use the chat area to ask questions and share resources. Only speak when given the opportunity by the host.
- Be respectful and considerate when providing your input both within the chat or verbally. Do not use inappropriate language.
- Use proper dress attire. Ensure you follow the district policy as you would during a regular working day.
- Do not eat or snack during virtual meetings. Professionalism should always be considered regardless if you are attending the meeting off site.
- Do not share employee or student confidential data.

User Expectations for Virtual Meetings - Educators

- Model safe practices and moderate student behavior during virtual meetings as you would in the classroom. Ensure you stipulate student expectations **prior** to engaging in virtual meetings, especially with parents.
- Do not discuss students' personal data at any point in time.
- Schedule virtual meetings with your students during school hours. Complete in a timely manner and share with your administrators. If a meeting must be scheduled after hours, ensure you first obtain approval from your administrators.
- Share teacher-created videos with students through your online platforms. Virtual meeting live videos should be screened to ensure that they do not contain inappropriate behavior or any personal student information **prior** to sharing.
- Follow all licensing and copyright guidelines when sharing educational resources, materials, videos, and/or activities with students.
- Do not take or record images of students for your own personal use.
- Do not leave online session for students to be able to join while teacher is not available. Utilize the pre-generated link provided through Google Classroom.

LAREDO INDEPENDENT SCHOOL DISTRICT
TECHNOLOGY
SERVICES DEPARTMENT

User Expectations for Virtual Meetings - Students



- Join a Google Meet link provided solely by a teacher, counselor, administrator, etc.
- Do not attempt to join a Meet that is shared by another student as you are only allowed to join Meet links that are intended for virtual classroom instruction or extracurricular activities.
- Be on time. Log in a few minutes prior to the meeting to ensure connectivity.
- Find a place with few distractions. No inappropriate materials should be visible or displayed.
- Turn on your camera and mute your microphone. Use the chat area to ask questions. Only speak when given the opportunity by your teacher, counselor, administrator, etc.
- Be respectful when using the chat box or speaking. Do not use inappropriate language.
- Use proper dress attire. Ensure you follow the district policy in regard to dress code.
- Do not eat or snack during virtual meetings.
- Do not take or record images of anyone within your virtual meetings.
- Only the intended student receiving instruction should be in attendance during the virtual meeting. At no point in time should a student share a Meet link within anyone.

LAREDO INDEPENDENT SCHOOL DISTRICT
TECHNOLOGY
SERVICES DEPARTMENT

Annual Cybersecurity Training Requirement

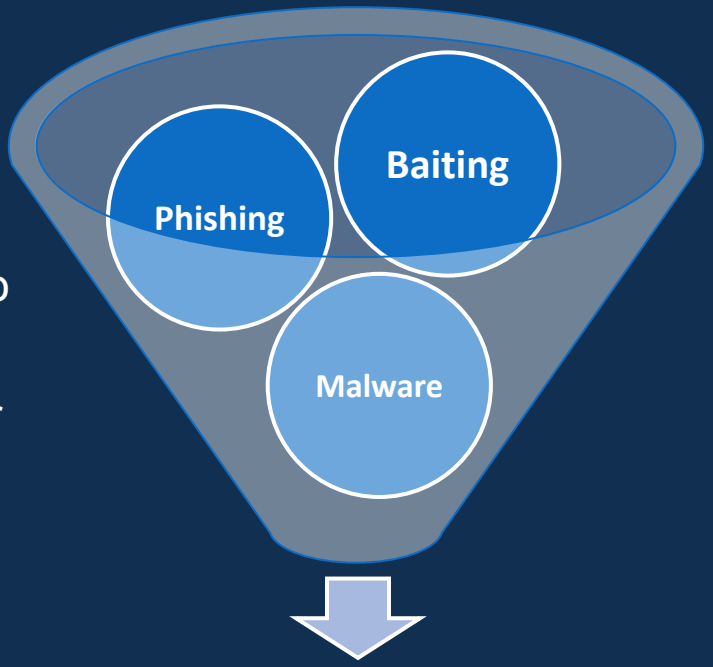
Cybersecurity is the protection of internet-connected systems, such as computers, servers, mobile devices, or networks, against unauthorized access to confidential, organization, personal, or any type of computerized data.

Laredo ISD **requires** all school district employees and elected officials who have access to a computer system or database, such as email, Skyward, Frontline, ClassLink, or any other district online program, for at least 25% of the employee's required duties to complete an annual certified cybersecurity training.

Information will be sent via email for completion of this annual requirement and all designated staff must comply to avoid disruption in access to district systems.

Social Engineering

Social engineering, as will be discussed within the cybersecurity training, is the art of manipulating people so they can give up confidential information, such as passwords, bank information, or access to your computer to secretly install spyware or other malicious software.



⚠ ALERT!! ⚠

- Use **strong** passwords!
- Use caution when opening emails coming from an outside organization, especially if it appears to be coming from an admin.!
- Do not open email attachments, click on unknown links, or download files from unexpected emails or text messages!
- Do not fall for phishing scams that say your account is in jeopardy!

*Note: The Technology Services Department will **NEVER** ask for your password over email. Be cautious of emails asking for personal information.

REPORT any suspicious emails to the Technology Services Department immediately by call (956) 273-1330.

LAREDO INDEPENDENT SCHOOL DISTRICT
TECHNOLOGY
SERVICES DEPARTMENT

LISD's Filtering System

Compliant with the Children's Internet Protection Act (CIPA) of 2001, LISD's Filtering System makes every effort to protect the user from accessing inappropriate material.

In an instance where a user *unintentionally* encounters something inappropriate within a site that contains adult, gambling, violence, or crime material, they must **immediately** discontinue access and contact their supervisor and the Technology Services Department.

LAREDO INDEPENDENT SCHOOL DISTRICT
TECHNOLOGY
SERVICES DEPARTMENT

Bring Your Own Devices (BYODs)

Employees and students are allowed to bring their own devices (BYOD) into the district and is a ***privilege.*** Individuals who use this privilege must also adhere to the district's Acceptable Use Policies.

*Note: Maintenance or technical issues related to BYODs is the **sole responsibility** of the student or employee possessing the device. The Technology Services Department does **not** address any issues pertaining to BYODs.

LAREDO INDEPENDENT SCHOOL DISTRICT
TECHNOLOGY
SERVICES DEPARTMENT

Student Training Requirements

As digital citizens, students will be granted access to use the district's technology resources through their designated/homeroom teacher by:

- completing the student internet safety training.
- having their parent/guardian sign a Student Agreement Form.
- verifying and activating their Skyward student account.

Teachers are responsible for making sure that students use the district resources and network in a manner aligned to their educational goals.

LAREDO INDEPENDENT SCHOOL DISTRICT
TECHNOLOGY
SERVICES DEPARTMENT

Audits and Monitoring

- LISD **will** periodically audit, inspect, and/or monitor **all** use of the district's technology resources, including, but not limited to, email and storage media as deemed appropriate.
- LISD **will** take disciplinary action if **any** violations of district policies and regulations are found.

LAREDO INDEPENDENT SCHOOL DISTRICT
TECHNOLOGY
SERVICES DEPARTMENT

Disciplinary Action

- ✔All district users must adhere to the district's Acceptable Use Policies (AUP) when utilizing the district's technology equipment and network/communication tools while participating in school-related and non-school related activities.

- ✔Violations of these policies will result in disciplinary action as stated in the Employee Handbook, Student Code of Conduct and User Agreements.

- ✔The severity of the violation committed will equal the degree of disciplinary action to be taken.

=

LAREDO INDEPENDENT SCHOOL DISTRICT
TECHNOLOGY
SERVICES DEPARTMENT

Disclaimer of Liability

In the case of an investigation concerning or relating to the misuse of the district's technology resources, the district will fully cooperate with local, state, or federal law enforcement agencies.

LAREDO INDEPENDENT SCHOOL DISTRICT
TECHNOLOGY
SERVICES DEPARTMENT

REMEMBER, as a district user…

- it is your responsibility to read and understand the full version of the district's Technology Acceptable Use Policies (AUP) posted on the www.laredoisd.org website.

- you must report any improper use of technology resources to your immediate supervisor and the Instructional Technology Department at (956) 273-1340.

- you must report any missing or modified files from your computer to the Technology Services Department at (956) 273-1330.

LAREDO INDEPENDENT SCHOOL DISTRICT
TECHNOLOGY
SERVICES DEPARTMENT

Enjoy your technology responsibly!

Thank you!

LISD LAREDO