

Lake Dallas ISD Technology Acceptable Use Policy

Introduction

Lake Dallas ISD recognizes that access to technology in school gives students greater opportunities to learn, engage, communicate, and develop skills that will prepare them for work, life, and citizenship. We are committed to helping students develop current technology and communication skills.

To that end, we provide training and access to technologies for student and staff use. Students and staff are trained annually on appropriate Internet and District network use.

This Acceptable Use Policy outlines the guidelines and behaviors that students and staff are expected to follow when using district-provided devices or when using personal devices at school facilities.

- The Lake Dallas ISD network is intended for educational purposes.
- There is no expectation of privacy. All activity over the network when using district-owned or personal devices may be monitored and retained.
- Access to online content via the network may be restricted in accordance with district policies and federal regulations, such as the Children's Internet Protection Act (CIPA).
- Students and staff are expected to follow the same rules for good behavior and respectful conduct online as offline.
- Misuse of school resources can result in disciplinary action.
- Lake Dallas ISD makes a reasonable effort to ensure the safety and security of staff and students online, but will not be held accountable for any harm or damages that result from use of school technologies.
- Users of the district network or other technologies are expected to alert Technology staff immediately of any concerns for safety or security

Technologies Covered

Lake Dallas ISD may provide Internet access, desktop computers, mobile computers or devices, videoconferencing capabilities, online collaboration capabilities, message boards, email, and more.

As new technologies emerge, Lake Dallas ISD will attempt to provide access to them, where they meet instructional needs, and/or the goals and objectives of the District Improvement Plan. The policies outlined in this document are intended to cover all available technologies, not just those specifically listed.

Usage Policies

All technologies provided by the district are intended for education purposes. All users are expected to use good judgment and to follow the specifics of this document as well as the spirit of it: be safe, appropriate, careful and kind; do not try to bypass technological protection measures; use good common sense; and ask if you don't know.

Internet Access

Lake Dallas ISD provides its users with access to the Internet, including web sites, applications, resources, content, and online tools. That access will be restricted in compliance with CIPA regulations and school policies. Internet usage may be monitored and activity records may be retained indefinitely.

Users are expected to respect that the school district employs the use of internet security filters as a safety precaution and should not try to circumvent them when accessing data on the internet. If a site or internet-based data is inaccessible and a user believes it should not be, the user should follow district protocol to alert a Technology staff member or submit the site for review. Unblock requests can be submitted directly from the blocked page, or through a School Dude ticket/request.

Third Party Accounts

In accordance with our district mission, goals, and our vision for technology, our students may require accounts in third-party systems. Many of these accounts will be used at school, for school-related projects, but may also be accessed outside of school as needed. These accounts typically come with additional, product-specific terms of use.

The use of these accounts will help our students master effective and proper online communications as required in the PreK - 12 Technology Applications Standards. The District reserves the right to administer third-party accounts for students. Examples of third-part accounts used by the district include, but are not limited to: Google Workspace for Education, Microsoft, Office 365, Apple, Destiny, Renaissance Place, Eduphoria, Moby Max, Edgenuity, Pearson, and My HRW.

Email

Lake Dallas ISD may provide students and staff with email accounts for the purpose of school related communication. Availability and use may be restricted based on school policies, or state / federal law.

If users are provided with email accounts, the district will provide email accounts hosted in Google, under Google's Workspace for Education product offering.

If users are provided with email accounts, they should be used with care. Users should not send personal information; should not attempt to open files or follow links from unknown or untrusted origin; should use appropriate language; and should only communicate with other people as

allowed by the district policy or the teacher. Prohibited uses of school-provided email include, but are not limited to:

- Sending personal information to any person or entity that is not directly related to the use or support of district curriculum and instruction, or school-sponsored activities
- Sending personal financial information, such as filing personal tax returns, applying for home mortgages, and applying for any sort of personal financial loan
- Signing up for service accounts that are not required by, or related to, the use or support of district curriculum and instruction, or school-sponsored activities. Examples include, but are not limited to:
 - Movies, music, shopping, social media or other accounts intended for personal use
 - Pornography
 - Dating sites
 - VPN hosting services
- Opening file attachments or clicking links that are of an unknown, or untrusted origin
- Using inappropriate language
- Communicating with other people or entities prohibited by district policy, or local, state, or federal law

LDISD Gmail accounts should not be used to sign up for personal, and/or extra-curricular services, without explicit authorization from LDISD Administration and/or the Technology department. Similarly, personal email accounts should not be used for LDISD business and instructional correspondence. In short, keep personal and school accounts and correspondence separate from one another.

All LDISD Gmail accounts used by *staff members* must have 2FA (two factor authentication) enabled. This is mandatory. (Student Gmail accounts do not have this requirement, but can be used with 2FA, if desired.)

Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Email usage may be monitored and archived.

Email Recovery Procedures

Lake Dallas ISD currently provides email accounts to district employees, which are hosted and archived by Google. The archiving of Lake Dallas ISD email is performed to comply with federal and state requirements pertaining to the retention of official school correspondence.

Consequently, any recovery of email from the Lake Dallas ISD email archive requires 1) a written request that includes the reason for the request, the staff/student accounts and/or subject

matter involved, the date range of the request, and 2) approval from a campus principal, department director, or superintendent-level personnel. The Superintendent, Executive Director of HR, and the Technology Director can facilitate email recovery, but the initial request must be submitted in writing, and approved by a principal, department director, or superintendent-level personnel before email recovery will be performed.

Cloud Storage

Lake Dallas ISD may provide students and staff with cloud storage (Google Drive, Microsoft OneDrive, iCloud, etc.) for the purpose of storing school-related files and correspondence. Availability and use may be restricted based on school policies. Cloud storage usage may be monitored and archived.

Social/Collaborative Content

Recognizing the benefits collaboration brings to education, Lake Dallas ISD may provide users with access to web sites or tools that allow communication, collaboration, sharing, and messaging among users.

Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Posts, chats, sharing, and messaging may be monitored. Users should be careful not to share personally-identifying information (PII), or other sensitive information online.

Mobile Devices Policy

Lake Dallas ISD may provide users with mobile computers or other devices to promote learning inside and outside of the classroom. Users should abide by the same acceptable use policies when using school devices off the school network as on the school network.

Users are expected to treat these devices with extreme care and caution; these are expensive devices that the school is entrusting to your care. Users should report any loss, damage, or malfunction to either the campus staff, or the Technology staff immediately. **Users may be financially accountable for any damage resulting from negligence or misuse.**

Use of school-issued mobile devices on and off of the school network may be monitored.

Security

Users are expected to take reasonable safeguards to protect the data that they use, and to do their part to help protect against external threats such as ransomware and viruses. This includes not opening or clicking web links contained in suspicious or unsolicited email, opening file attachments without verifying their source or integrity, or launching applications of unknown or untrusted origin.

If you believe a computer or mobile device you are using might be infected with a virus or other form of malware, please alert Technology. Do not attempt to remove the virus yourself or download any programs to help remove the virus.

Users are also expected to safeguard their account passwords, and change them at least as often as required by district system policy, or more frequently, if desired. Account passwords should be protected, not shared with others, and not written down. Be aware of your surroundings as you enter passwords, and take steps to ensure your password is protected, and not easily observed by others.

Approval Required for Software and Curriculum Resource Use

All employees are reminded that any software or curriculum resources intended for use must first be approved by the following:

- Your direct supervisor
- Your applicable department Director
- The Technology Department

Most requests for approval can be submitted through Incident IQ. This process helps ensure compatibility, data privacy compliance, and alignment with district instructional goals. If you have any questions regarding this process or are unsure how to proceed, please consult with your direct supervisor.

Investigations

Any requests related to accessing private information or student/staff account information must be directed to the District Cybersecurity Coordinator (the LDISD Director of Technology).

The Cybersecurity Coordinator must be present for all investigations involving the recovery of digital evidence. This protocol is in place to ensure the integrity of digital investigations and the protection of sensitive data in compliance with district policies and applicable laws.

Unauthorized access or attempts to conduct such investigations without proper authorization is prohibited.

Downloads

Users should not download, or attempt to download or run, executable programs over the school network or onto school resources without explicit permission from Technology staff.

You may be able to download other file types, such as images or videos. For the security of our network, download such files only from reputable sites, and only for education purposes.

Use of @ldisd.net domain

The @ldisd.net domain is registered for sole use by Lake Dallas ISD. You are not authorized to create any personal hardware system or software application, or user account which utilizes this domain name.

Netiquette

Users should always use the Internet, network resources, and online sites in a courteous and respectful manner.

Users should also recognize that among the valuable content online is unverified, incorrect, or inappropriate content. Users should use trusted sources when conducting research via the Internet.

Users should also remember not to post anything online that they wouldn't want parents, teachers, or future colleges or employers to see. Once something is online, it's out there—and can sometimes be shared and spread in ways never intended.

Plagiarism

Users should not plagiarize (or use as their own, without citing the original creator) content, including words or images, from the Internet. Users should not take credit for things they didn't create themselves, or misrepresent themselves as an author or creator of something found online. Research conducted via the Internet should be appropriately cited, giving credit to the original author.

Personal Safety

Users should never share personal information, including phone number, address, social security number, birthday, or financial information, over the Internet without adult permission. Users should recognize that communicating over the Internet brings anonymity and associated risks, and should carefully safeguard the personal information of themselves and others. Users should never agree to meet someone they meet online in real life without parental permission.

If you see a message, comment, image, or anything else online that makes you concerned for your personal safety, bring it to the attention of an adult (teacher or staff if you're at school; parent if you're using the device at home) immediately.

Cyberbullying

Cyberbullying will not be tolerated. Harassing, dissing, flaming, denigrating, impersonating, outing, tricking, excluding, and cyberstalking are all examples of

cyberbullying. Don't be mean. Don't send emails or post comments with the intent of scaring, hurting, or intimidating someone else.

Engaging in these behaviors, or any online activities intended to harm (physically or emotionally) another person, will result in severe disciplinary action and loss of privileges.

In some cases, cyberbullying can be a crime. Remember that your activities are monitored and retained.

Examples of Acceptable Use

I will:

- ✓ Use school technologies for school-related activities.
- ✓ Follow the same guidelines for respectful, responsible behavior online that I am expected to follow offline.
- ✓ Treat school resources carefully, and alert staff if there is any problem with their operation.
- ✓ Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies.
- ✓ Alert a teacher or other staff member if I see threatening, inappropriate, or harmful content (images, messages, posts) online.
- ✓ Use school technologies at appropriate times, in approved places, for educational pursuits.
- ✓ Cite sources when using online sites and resources for research.
- ✓ Recognize that use of school technologies is a privilege and treat it as such.
- ✓ Be cautious to protect the safety of myself and others.
- ✓ Help to protect the security of school resources.
- ✓ Notify district or campus administration and/or the Technology department staff if I discover misuse of district network resources and information.
- ✓ Comply with the policies listed in the Lake Dallas ISD - BYOD Program guide, as applicable
- ✓ Comply with the policies listed in the Lake Dallas ISD Mobile Device Guide, as applicable

This is not intended to be an exhaustive list. Users should use their own good judgment when using school technologies.

Examples of Acceptable Use

I will not:

- Use wireless hotspots on the LDISD network that have not been provided to me by the district
- Connect personal wireless routers, switches, access points, firewalls, and other related network equipment to the LDISD network
- Use personal computing devices on the LDISD network that have not been approved for use by authorized personnel
- Use school technologies in a way that could be personally or physically harmful, to myself or others
- Deliberately damage or misuse school devices and property
- Attempt to find inappropriate images or content
- Plagiarize content I find online
- Use language online that would be unacceptable in the classroom
- Engage in cyberbullying, harassment, or disrespectful conduct toward others •

Agree to meet someone I meet online in real life

- Use school or personal technologies for illegal activities or to pursue information on such activities while at school, whether on or off the school network
- Obtain user or system account credentials through illicit means
- Use another individual's account, not assigned to me, or without explicit authorization, for any reason
- Use software and/or hardware designed for the purpose of network reconnaissance •
- Circumvent, or attempt to circumvent the school's safety/security measures and filtering tools
- Use school or personal technologies to send malicious or unauthorized email •
- Attempt to illicitly access, use or sabotage any district system or application and data content
- Access, modify, copy, transmit, or view any education record in a manner which violates district policies, or local, state or federal laws

This is not intended to be an exhaustive list. Users should use their own good judgment when using school technologies.

Limitation of Liability

Lake Dallas ISD will not be responsible for damage or harm to persons, files, data, or hardware. While Lake Dallas ISD employs filtering and other safety and security mechanisms, and attempts to ensure their proper function, it makes no guarantees as to their effectiveness. Lake Dallas ISD will not be responsible, financially or otherwise, for unauthorized transactions conducted over the school network.

Biometric Acknowledgment:

The district reserves the right to use a form of identification for each device called biometrics. This is similar to your child utilizing their fingerprint to access their lunch account when going through the lunch serving lines. The system does not store your child's fingerprint. With your signature below you are giving consent for your child to utilize biometrics to sign into their Apple device.

Violations of this Acceptable Use Policy

- Restricted use of network, technology, or computer privileges
- Suspension of network, technology, or computer privileges
- Notification to parents (if a student)
- Detention or suspension from school and school-related activities
- Suspension of duties (if an employee of the district)
- Confiscation of any device, regardless of ownership, that is suspected of involvement with any violations of this AUP
- Liability for cost to diagnose and repair any damage or loss caused by any violation of this AUP
- Termination of employment, in accordance with LDISD policies and applicable laws
- Legal action and/or prosecution

For questions or concerns, please contact your school's technology support team or administration at ghamilton@ldisd.net.

Exhibit A: Device Fees for lost or damaged items

Apple Device Fees		
Accidental damage from handling resulting from an unexpected and unintentional external event (such as, drops and damage caused by liquid contact)	First Occurrence	No Fee
Accidental damage from handling resulting from an unexpected and unintentional external event (such as, drops and damage caused by liquid contact)	Second Occurrence	No Fee
Accidental damage from handling resulting from an unexpected and unintentional external event (such as, drops and damage caused by liquid contact)	Third or more Occurrences	Cost to repair/replace the device
Intentional damage from a direct action from the student resulting damage.	First Occurrence	50% of the cost to repair/replace the device
Intentional damage from a direct action from the student resulting damage.	Second or more Occurrences	Cost to repair/replace the device
A device that is lost or not returned to the district		Cost to replace the device