



THINK. PROTECT. RESPECT.

A Student and Family Guide to Responsible Technology Use

Technology should support learning, protect people and information, and strengthen our school community.

1

USE IT TO LEARN



Use District technology for schoolwork, research, communication, creativity, and activities approved by staff.

- Stay focused on learning.
- Personal use must not distract others or disrupt instruction.

2

PROTECT YOURSELF



Keep accounts, passwords, personal information, and devices secure.

- Use only your assigned accounts and devices.
- Report lost devices, suspicious messages, or compromised accounts right away.

3

RESPECT OTHERS



Communicate in ways that are safe, kind, honest, and appropriate.

- Do not bully, threaten, harass, impersonate, or discriminate.
- Do not share private, hateful, explicit, violent, or disruptive content.

4

CREATE RESPONSIBLY



Use digital tools in ways that honestly represent your learning.

- Follow teacher directions for AI & digital tools.
- Cite sources, respect copyright, and ask before recording or sharing others.

5

PROTECT OUR SYSTEMS



Care for devices and help keep District systems safe.

- Do not bypass filters, use unauthorized VPNs or hotspots, or install unapproved software.
- Report damage, technical problems, or inappropriate content immediately.

6

FOLLOW DIRECTIONS & SPEAK UP



Follow staff directions about when, where, and how technology may be used.

- Put devices away or surrender them when directed under school procedures.
- Tell a trusted adult about cyberbullying, threats, security concerns, or misuse.



KNOW ABOUT PRIVACY

Students should not expect privacy when using District devices, accounts, applications, or networks. Use may be monitored or reviewed to maintain safety, protect systems, investigate concerns, and enforce school rules.



CHOICES HAVE CONSEQUENCES

Responses may include reteaching, family notification, supervised or restricted access, financial responsibility for damage, discipline, or referral to law enforcement when appropriate. Serious conduct may result in immediate consequences.

PAUSE BEFORE YOU POST • PROTECT YOUR INFORMATION • CHOOSE RESPECT

Read the complete Student Acceptable Use of District Technology Agreement and related resources on the District website.

BEFORE YOU CLICK, POST, SHARE, OR SEND - ASK:



THINK

Is it for learning?



PROTECT

Is it safe and private?



RESPECT

Is it kind and appropriate?



Los Alamitos Unified School District

Student Acceptable Use of District Technology Agreement

Los Alamitos Unified School District provides students with access to technology, digital resources, online instructional services, and internet connectivity to support learning, communication, creativity, collaboration, and college and career readiness.

Students are expected to use these resources safely, responsibly, ethically, and for educational purposes. This agreement applies whenever a student uses:

- A District-issued device;
- A District account, network, application, or online service;
- A personally owned device connected to a District network or used during a school activity; or
- Technology for communicating or creating content that affects the school environment.

School rules, the Student Code of Conduct, Board policies, and applicable laws continue to apply when students use technology.

Student Responsibilities

When using District technology, students agree to:

1. Use Technology for Learning

Use District technology primarily for school assignments, research, communication, collaboration, and other activities authorized by a teacher or District employee.

Limited personal use may be permitted when it does not interfere with learning, school operations, network performance, or the rights of others.

2. Protect Accounts and Personal Information

Students must:

- Use only the accounts and devices assigned or authorized for them;
- Keep passwords and login information private;
- Log out or secure devices when not in use;
- Protect personal information such as addresses, phone numbers, passwords, identification numbers, and location information;
- Never attempt to access another person's account, files, messages, or data; and
- Immediately report a lost device, compromised account, suspicious message, or security concern.

Students are responsible for activities conducted through their assigned accounts unless the account or device has been reported as compromised.

3. Communicate Respectfully

Students must communicate in a manner that is respectful, appropriate, and consistent with school expectations.

Students may not use technology to:

- Bully, harass, intimidate, threaten, embarrass, or discriminate against another person;
- Share hateful, obscene, sexually explicit, violent, or substantially disruptive content;

- Impersonate another person or misrepresent an individual or organization;
- Knowingly create or distribute false, defamatory, deceptive, or misleading information; or
- Share private information, images, recordings, or communications without authorization.

These expectations apply to conduct occurring on campus and to off-campus conduct when it causes, or is reasonably likely to cause, a substantial disruption to school activities or the rights and safety of others.

4. Use Digital Content Responsibly

Students must respect copyright, licenses, intellectual property, and academic integrity requirements.

Students may not:

- Copy, download, distribute, or publish protected content without permission or proper attribution;
- Use technology to cheat, plagiarize, fabricate information, or misrepresent work as their own;
- Record, photograph, or publish another person without authorization when privacy would reasonably be expected; or
- Use artificial intelligence or other digital tools in a way that violates teacher directions, assignment requirements, academic integrity expectations, or District guidelines.

Students should clearly identify or cite outside sources, including artificial intelligence tools, when required by their teacher.

5. Protect District Systems and Equipment

Students must handle District devices and equipment carefully and follow all checkout, storage, charging, transportation, and return procedures.

Students may not:

- Intentionally damage, alter, disable, or interfere with a device, network, application, account, or security system;
- Bypass or attempt to bypass internet filters, monitoring systems, device restrictions, or other security controls;
- Install unauthorized software, applications, browser extensions, virtual private networks, proxy services, or hardware;
- Introduce viruses, malicious software, or other harmful code;
- Attempt to gain unauthorized access to a system, account, network, or confidential information;
- Change device settings or configurations without permission; or
- Use District technology for commercial activity, unlawful conduct, or other purposes unrelated to the District's educational mission.

Accidental damage, technical problems, or unintended access to inappropriate content should be reported immediately to a teacher, administrator, or other District employee.

6. Follow Staff Directions

Students must follow the directions of teachers and staff regarding when, where, and how technology may be used.

Students must close, silence, put away, or surrender a device when directed by an authorized staff member in accordance with school and District procedures.

District Monitoring and Student Privacy

District technology, accounts, networks, and data created, transmitted, received, or stored through District systems are District resources.

Students should not expect communications, searches, files, browsing activity, or other use of District technology to be private.

The District may monitor, access, review, preserve, or disclose technology use when reasonably necessary to:

- Maintain student and staff safety;
- Protect District systems, devices, accounts, and data;
- Investigate suspected misconduct or security concerns;
- Maintain and troubleshoot technology services;
- Comply with legal requirements, records requests, or court orders; or
- Enforce Board policy, school rules, and this agreement.

The District uses internet filtering and other safeguards as required by law. However, no filtering system can prevent access to all inappropriate, inaccurate, or harmful content. Students who unintentionally access inappropriate content must leave the content and report it to a staff member.

Additional filtering information is available at: <https://www.losal.org/webfilter>

Online Instructional Services

The District uses approved online instructional services to provide curriculum, communication, collaboration, assessment, accessibility, and personalized learning opportunities.

These services may require the District to provide limited student information, such as:

- Student name;
- District email address;
- Student identification number;
- School, grade level, or class enrollment; and
- Information generated through the student's use of the educational service.

The District reviews applications and services for compliance with applicable student privacy, security, and education laws.

BYOD - Personally Owned Devices

Students who bring personally owned devices to school do so at their own risk. The District is not responsible for the loss, theft, damage, maintenance, or support of personally owned devices.

When a personal device is used on campus, during a school activity, or to access District technology, the student must follow this agreement and all school rules.

Students must:

- Use only authorized District network access while on campus;
- Follow teacher and staff directions regarding device use;
- Keep the device secure and appropriately charged; and
- Abstain from using personal hotspots, proxy services, virtual private networks, or other methods to bypass District safeguards.

A personal device may be restricted or temporarily held in accordance with school procedures when it is used in violation of school or District rules.

Additional BYOD personal-device information is available at: <https://www.losal.org/byod>

Reporting Safety or Security Concerns

Students must promptly report:

- Cyberbullying, threats, harassment, or concerning digital communications;
- Lost or stolen devices;
- Compromised passwords or accounts;
- Suspected unauthorized access;
- Inappropriate content received or unintentionally accessed;
- Damage to District equipment; or
- Any security weakness or misuse of District technology.

Students should report concerns to a teacher, counselor, administrator, technology staff member, or another trusted District employee.

Students should not investigate a security concern themselves, forward harmful content, or delete relevant evidence unless directed to do so by a District employee.

Consequences for Misuse

Violations will be addressed based on the student's age, the nature and severity of the conduct, the student's disciplinary history, the impact on others, and applicable laws and District policies.

Possible responses include:

1. Reteaching expectations, a warning, or a restorative response;
2. Parent or guardian notification;
3. Temporary restriction of a device, account, application, network, or other technology privilege;
4. Required supervision or limitations on future technology use;
5. Restitution or financial responsibility for intentional, reckless, or negligent loss or damage, as permitted by law;
6. School disciplinary action, including suspension or expulsion when authorized by law and Board policy;
7. Referral to law enforcement or another agency when required or appropriate; and
8. Civil or criminal consequences when applicable.

The loss of access to technology will be carefully considered, as it is an important part of instruction. When access is restricted, the school will determine how the student will continue to participate in required learning activities.

Serious conduct may result in immediate consequences without first using less restrictive interventions. This includes conduct involving credible threats, significant harassment, unauthorized access, intentional damage, distribution of sexually explicit content, or actions that compromise student safety or District systems.

Student Acknowledgement

I have read and understand the Student Acceptable Use of District Technology Agreement.

I agree to:

- Use technology safely, responsibly, ethically, and for educational purposes;
- Protect my account, personal information, and District equipment;
- Communicate respectfully;
- Follow staff directions;
- Report safety, security, and technology concerns; and
- Accept the consequences that may result from misuse.

I understand that I should not expect privacy when using District technology and that my use may be monitored or reviewed.

Student Name: _____

Student Signature: _____

Date: _____

Parent or Guardian Acknowledgement and Consent

I have reviewed this agreement with my student and understand the expectations governing the use of District technology, accounts, networks, applications, online instructional services, and personally owned devices used at school.

I understand that:

- Technology and online instructional services are an integral part of the District's educational program;
- The District uses reasonable safeguards, including internet filtering, monitoring, staff supervision, and application review, but cannot guarantee that all inappropriate or inaccurate content will be inaccessible;
- My student's use of District technology may be monitored, accessed, reviewed, or retained as described in this agreement;
- The District may provide limited student information to approved online instructional services for legitimate educational purposes;
- Personally owned devices are brought to school at the owner's risk;
- I may be financially responsible, as permitted by law, for intentional or negligent loss of or damage to District property; and
- Violations may result in restrictions, disciplinary action, restitution, referral to law enforcement, or other consequences.

I authorize my student to use District technology, internet access, District accounts, and District-approved online instructional services for educational purposes.

Parent/Guardian Name: _____

Parent/Guardian Signature: _____

Date: _____

Student Name: _____

School: _____

Grade: _____

Related District Resources:

The following detailed guidance is incorporated by reference and maintained on the District website:

- [Board Policy 6163.4 – Student Use of Technology](#)
- [Board Administrative Regulation 6163.4](#)
- [BYOD Internet Filtering & Certificate Installation Information](#)
- [Cyberbullying, Harassment, and Digital Citizenship Resources](#)
- [Los Alamitos High School Chromebook 1:1 Program Information](#)
- [Personal Device and BYOD Guidance](#)