Los Alamitos Unified School District
Acceptable Use Agreement of District Technology

Student pledge (K-12)

Electronic information resources offer multiple opportunities of educational value. Los Alamitos Unified supports access by students to rich information resources and encourages students to develop the information research skills necessary to analyze and evaluate such resources. I understand and will follow the rules of this contract to be a responsible digital citizen. I understand that any violations of the *attached* "Acceptable Use of District Technology" may result in disciplinary action, losing my privileges, and appropriate legal action. I also agree to report any misuse of the system to a staff member. Misuse can come in many forms, but can be viewed as any material sent, received, or displayed that indicates or suggests pornography, unethical or illegal solicitation, racism, sexism, inappropriate language, and other inappropriate content while using district technology or privately owned wireless and/or portable electronic equipment during school hours, during a school activity or on a school account. All of the rules of behavior described in the school code apply.

Parent or Guardian

As the parent or guardian of this student, I have read this contract and understand that the use of electronic resources is designed for educational purposes only. I understand that it is impossible for the District to restrict access to all controversial materials, and I will not hold the District responsible for materials acquired on the network. I give my permission for my child's work to be published on the District's Internet World Wide Web server. I give permission for my child to use District approved apps and online resources that meet State, Federal, and student safety and privacy legal requirements (for an updated list of resources, please visit: **http://www.losal.org/BYOD**). I understand that the District cannot protect my child's work against unauthorized uses or copyright violations. I hold the District harmless from any damages, awards, or claims of liability resulting from my child's access to technology in instruction. I also agree to report any misuse of the system to school personnel. Misuse can come in many forms, but can be viewed as any material sent, received or displayed that indicates or suggests pornography, unethical or illegal solicitation, racism, sexism, inappropriate language, and other inappropriate content described above while using district technology or privately owned wireless and/or portable electronic equipment during school hours or during a school activity. Should my child breach the guidelines, he/she will lose computer privileges and that such breach may result in disciplinary action. I agree to allow my child to have access to the internet. By clicking "Yes," I agree to the Board Policy 6163.4 and the attached "Acceptable Use of District Technology".

Los Alamitos Unified School District
Acceptable Use of District Technology

We are pleased to announce that electronic information services are available to support information resources and encourage students to develop the information research skills necessary to analyze and evaluate such. The District strongly believes in the educational value of electronic services and recognizes their potential to support our curriculum and student learning in our district. Our goal in providing this service is to promote educational excellence by facilitating resource sharing, collaboration, innovation and communication.

The District will make every effort to protect students from any misuses or abuses as a result of their experiences with an information service. All users must be continuously on guard to avoid inappropriate and illegal interaction with the information service.

District Regulation

District technology includes, but is not limited, to the District's Internet/Intranet/Extranet-related systems, email system, Microsoft and Google school accounts, school cloud and remote learning phone system including voice mail, cell phones, MP3 player, iPods, iPads, Google Classroom, wireless communication, video conferencing, blogs, computers, the computer network including Internet access through the network, storage media, and office equipment. Use of District technology by each and every employee, student, volunteer, contractor, or other individual shall constitute that person's acknowledgment of agreement to abide by this regulation. District technology, including the data and products of its use, is the property of the District.

A. The District reserves the right to monitor the use of District technology without notice and consent to ensure that:
    1. Safety for all stakeholders is maintained.
    2. Public resources are appropriately used for District-related business.
    3. Applicable District policies and regulations, including those regarding harassment and nondiscrimination, are followed.
    4. Any personal use of District technology does not interfere with District business or job duties and is minimal in terms of use and cost.

B. The District may require new registration, account information or password changes from any person to continue services, either on a regular basis or without notice. Passwords should not be given to any individual except authorized District personnel and supervisors. Users shall not login as others using their personal user ID or password credentials.

C. Users of District technology shall not have an expectation of privacy in any matter created, received, stored in, or sent from District technology, including password-protected matter, all of which may be public records.

D. A parental approval form is required for each student allowed access to office technology, specific computers, or the Internet. Parents and students shall be provided with Board Policy 6163 describing how students will be expected to use the equipment and what will constitute unacceptable behavior.

E. Students shall report all incidents of unacceptable use immediately without inquiry to their teachers and school administrators.

F. You may use District Technology only for class assignments or for personal research on subjects similar to what you might study in a class or in the school library. Use for entertainment purposes, such as but not limited to personal blogging, instant messaging, on-line shopping, video streaming, video downloads, or gaming is not allowed.

G. Unauthorized staff, volunteers, parents, family members, or significant others may not configure, diagnose, or repair any District equipment. Only District approved personnel shall be authorized to perform this work. The Los Alamitos High School's Student Tech Team may assist authorized District personnel in diagnosing and performing minor authorized repairs with prior approval of the Director of IT and Los Alamitos High School administrators under the guidance of an IT Department staff member.

H. Security systems that are not approved by the District are strictly prohibited; i.e., CMOS passwords, unapproved wireless access points, or third party security applications. If such systems are discovered, the equipment shall be erased and reconfigured to meet District standards and may result in disciplinary action.

I. Prohibited uses of District technology include the following:

1. Using District technology for commercial advertising, gain, fraud, or unauthorized personal or non-profit purposes;
2. Political or religious activities not directly related to assigned school projects;
3. Intentionally disabling or bypassing security systems or procedures;
4. Unauthorized use of another's passwords or computer to access files, resources or systems, or unauthorized use of an account belonging to another user;
5. Unauthorized access to protected and confidential data systems containing student, personnel, financial, or other data;
6. Using District computers to copy software or using software in violation of copyright or license agreements;
7. Copying District software, files or documents for personal use or downloading or installing personal software on District computers for non-District purposes;
8. Unauthorized use or possession of services, real property, or intellectual property;
9. Sending, creating, intentionally receiving or storing any material in violation of any United States or California laws or District policy. Such material includes, but is not limited to:
    i. Copyrighted, trademarked, or patented material;
    ii. Inaccurate, disruptive, threatening, racist, or discriminatory, sexist or obscene material.
    iii. Any material that could be construed as harassment or disparagement of others based on their race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs;
    iv. Material protected by privilege, trade secret, privacy, or confidentiality laws;
    v. Material that depicts violence or death or promotes weapons;
    vi. Material that is designated as "adults only";
    vii. Material that promotes the use of alcohol, tobacco or illegal drugs;
    viii. Material that promotes school cheating;
    ix. Material that advocates participation in hate groups or other potentially dangerous groups.
10. Using District technology to either create a computer virus or other malicious software or to knowingly initiate a computer virus or other malicious software on the network or other District technology, or any other processes that would damage computers, computer systems or computer networks;
11. Intentionally disrupting network traffic or degrading or disrupting equipment and system performance;
12. Accessing or exploring the internet, chat rooms, social media (i.e. Facebook, Instagram, Twitter, etc.,), or unauthorized online games that do not support the curriculum and/or are inappropriate for school-related work;
13. Vandalizing and/or tampering with equipment, programs, data, system performance, or other components of the network, including copying, distributing, or modifying copyrighted software;
14. Attempting to infiltrate or "hack" into any technological system, or interfering with another person's ability to use that system
15. Posting anonymous messages, unapproved web pages, or unlawful or libelous information on the system;
16. Granting remote or local control of a networked system to a third party.

J. Technology equipment (hardware or software) that has an instructional emphasis may not be taken, or copies to be taken, home or off-site without written permission signed by a District administrator.

K. If you mistakenly access inappropriate information, you should immediately report this access to a teacher or school administrator. This will protect you against a claim that you have intentionally violated this policy.

L. You should promptly disclose to your teacher or school staff any message or other materials you receive that are inappropriate or make you feel uncomfortable. You should not delete this information unless instructed to do so by a staff member.

M. It is important for you to protect your personal contact information, which includes your full name, together with other information that would allow an individual to locate you, including your family name, your home address or location, your work address or location, or your phone number.

N. Personal or non-district purchased hardware and software will not be allowed to connect or integrate into the district network unless stipulated by another board regulation, authorized as part of a district authorized school-based "bring your own device" (BYOD) program, or authorized by District personnel for educational purposes.

O. Consequences for violations of the policy or regulation include the following:
   1. Suspension or revocation of access to District technology;
   2. Suspension or revocation of network privileges, including email;
   3. Disciplinary action, up to and including termination;
   4. Civil or criminal action against the offender, where appropriate.
   5. Your parents can be held financially responsible for any harm that may result from your intentional misuse of District or Personal Technology.

Children's Internet Protection Act

A. In compliance with the Children's Internet Protection Act, the District is utilizing the K – 12 installed filtering or blocking software to restrict access to Internet sites containing material harmful to minors. The software works by scanning for objectionable words or concepts, as determined by the School District. However, no software is foolproof. A user who incidentally connects to an inappropriate site must immediately disconnect from the site and notify a teacher or supervisor. If a user sees another user accessing inappropriate sites, he or she should notify a teacher or supervisor immediately.

B. Students and staff may not disable or bypass the District's filtering software at any time when students are using the Internet system if such disabling will cease to protect against access to inappropriate materials. Authorized staff may temporarily or permanently unblock access to sites containing appropriate material if the filtering software has inappropriately blocked access to such sites.

C. Staff must supervise student use of the District Internet system, in a manner that is appropriate to the students' age and the circumstances of use.

D. The following restrictions against inappropriate speech and messages apply to all speech communicated and accessed through the District Internet system, including all e-mail, instant messages, Web pages, and Web logs. Students shall not send obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful messages. Students shall not post information that could cause damage, danger, or disruption, or engage in personal attacks, including prejudicial or discriminatory attacks. Students shall not harass or bully another person, or knowingly or recklessly post false or defamatory information about a person or organization.

E. Students' home and personal Internet use can have an impact on the school and on other students. If students' personal Internet expression - such as a threatening message to another student or a violent website - creates a likelihood of material disruption of the school's operations, students may face school discipline and criminal penalties.

Cyberbullying

A. 'Cyberbullying' includes, without limitation, the transmission of communications, posting of harassing messages, direct threats, social cruelty, or other harmful texts, sounds or images on the Internet, social networking sites, or other digital technologies using a telephone, computer, or any wireless communication device.

B. Cyberbullying includes knowingly or recklessly posting or sharing false or defamatory information about a person or organization; posting or sharing private information about another person that is private; posting or sharing inappropriate or obscene photographs of other people; breaking into another person's electronic account and/or assuming that person's identity in order to damage that person's reputation or friendships, e.g., fake social media profiles.

C. Cyberbullying using District or Personal Technology is prohibited, when the District reasonably believes the conduct or speech will cause actual, material disruption of school activities. The term "Cyberbullying" will not be interpreted in a way that would infringe upon a student's right to engage in legally protected speech or conduct.

D. Cyberbullying and sexting are strictly prohibited. Our District takes bullying and harassment very seriously. Students shall not use any Internet or other communication device to intimidate, bully, harass, or embarrass other students or staff members. Students who engage in such activity on school grounds or who engage in such activity off campus and create a material disruption of school operations shall be subject to penalties for bullying and harassment contained in the student handbook, as well as possible criminal penalties.

E. All students or others who experience, witness or become aware of Cyberbullying shall immediately report it to a teacher or District administrator.

Email and Messaging

A. All electronic mail messages, like all paper documents, are the property of the District and are subject to office policy, procedures, and control. As such, email messages are subject to discovery in any legal proceedings.

B. Email is for educational purposes only – not personal use. Email is not a confidential forum for communications. The contents of messages may be monitored without notice or consent, and all users should be aware that every message can be stored, forwarded and printed.

C. Email messages should not contain profanity, racial or sexual slurs, or other unprofessional language.

D. Unauthorized use, or forging, of email header information and creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type is prohibited.

BYOD Student/Parent Agreement

Students learn collaboration, communication, creativity and critical thinking in a variety of ways throughout the school day. In an effort to increase access to those 21st Century skills, Los Alamitos Unified School District will allow personal devices on our guest network and school grounds for students who follow the responsibilities stated in the Acceptable Use Policy and the guidelines regarding Bring Your Own Device (BYOD). Furthermore, the student must agree to the following conditions:

A. Only the BYOD Internet access/gateway provided by the school may be accessed while on campus. Personal Internet connective devices such as, but not limited to, cell phones, cell network adapters (MiFi), or other unfiltered "hot spots" are not permitted to be used to access outside Internet sources at any time. Los Alamitos Unified School District follows the safeguards of the Federal Children Internet Protection Act (CIPA) laws to mitigate access to any obscene or harmful Internet material in our District. Students attempting to bypass our Internet filters or using 3G/4G/LTE technologies may result in disciplinary actions.

B. The student device must be fully charged upon arrival because the school cannot guarantee charging access.

C. The student complies with teachers' request to shut-down the device or close the screen.

D. The student take full responsibility for his or her technology device. The District is not responsible for the security of student-owned technology.

E. The school district reserves the right to inspect a student's personal device if there is reason to believe that the student has violated Board policies, administrative procedures, school rules or has engaged in other misconduct while using their personal device, especially as it relates to bullying or cyberbullying or source of a computer virus.

F. Failure to adhere to this agreement may result in the student's device being confiscated and delivered to the Principal's office for the day, banned from using the device in the classroom/school, and disciplinary actions.

Warranties of Security or Services

The Los Alamitos Unified School District makes no warranties of any kind, whether expressed or implied, for District technologies, including network services. District will not be responsible for any damages or losses suffered while using District technologies. These damages include loss as a result of delays, non- or mis-deliveries, or service interruptions caused by the system, errors, or omission. Use of any information obtained via the network is at the individual's own risk. District specifically disclaims responsibility for the accuracy of information obtained through its network services.

Users may encounter material on the Internet that is controversial and which user, parents, teachers, or administrators may consider inappropriate or offensive. It is the user's responsibility not to initiate access to such material. Any efforts by District to restrict access to Internet material shall not be deemed to impose any duty on District to regulate access to material on the Internet. The District makes no warranties with respect to network services, particularly the Internet, and specifically assumes no responsibilities for:

A. The content of any advice or information received by a user from a source outside the county or any costs or charges incurred as a result of seeking or accepting such advice;

B. Any costs, liabilities or damages caused by the way the user chooses to use network access;

C. Any consequences of service interruptions or changes, even if these disruptions arise from circumstances under the control of the District.