

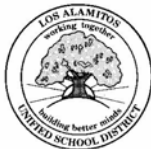
Print Name: _____
Student to print - Last name, First name

Signature: _____
Student Signature

Date: _____

Year of Graduation: June

MUST BE TURNED IN AT REGISTRATION



**Los Alamitos Unified School District
Policy and Regulations for Acceptable Use of District Technology**

Student pledge (K-12)

I understand and will follow the rules of this contract. I understand that any violations of the *attached* "Acceptable Use of District Technology Policy and Regulations" 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. All of the rules of behavior described in the school code apply.

Parent or Guardian

Students under the age of 18 must also have the signature of a parent or guardian who has read this contract. 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 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. Should my child breach the guidelines, he/she will lose computer privileges and that such breach will result in disciplinary action. I agree to allow my child to have access to the internet.

Print Name: _____
Parent/Guardian to print name

Signature: _____
Parent/Guardian Signature

Date: _____

PLEASE COMPLETE AND RETURN PAGE 1 TO YOUR SCHOOL



Los Alamitos Unified School District Acceptable Use of District Technology Policy and Regulations

We are pleased to announce that electronic information services are now available to students and teachers in our District who qualify as a result of participation in an orientation or training course. The District strongly believes in the educational value of such 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, innovation and communication.

The District will make every effort to protect students and teachers 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.

Please read this document carefully. When signed by you and, if appropriate, your guardian/parent, it becomes a legally binding contract. We must have your signature and that of your guardian/parent before we can provide you with an access account.

District Policy

The Governing Board recognizes and supports advances in technology. While these technologies provide a valuable resource to the District, it is important that the District's use of technology be appropriate for District purposes. In effect, inappropriate use may result in loss of employee and student productivity, service, compromised security, lost data, and other negative consequences.

District technology includes, but is not limited to, the District's internet-, intranet-, and extranet-related systems; email system; phone system including voice mail; video conferencing; computers, the computer network, including Internet access through the network; storage media; and office equipment. In order to minimize risk to the District, confidential information about students, employees, or District operations shall not be transmitted outside of the District without authorization. Confidential data are housed on separate servers in which student access is not permitted; staff access may be permitted only with prior authorization.

Use of District technology by each and every employee, student, volunteer, contractor, or other individual shall constitute that person's acknowledgment of and agreement to abide by this policy. District technology is the property of the District. Use of District technology is a privilege, not a right. Users of District technology shall not have an expectation of privacy in their use of District technology. The District reserves the right to monitor use of District technology to ensure public resources are appropriately used for District-related business and to ensure that the District's policies and regulations regarding harassment and nondiscrimination, as well as other applicable policies and regulations, are being followed. Any use of District technology for personal use must be minimal and not interfere with District business or job duties.

Users of District technology shall not engage in prohibited uses, as defined in Administrative Regulation. Any violations of this policy or regulation shall result in consequences up to and including disciplinary, civil, and/or criminal action.

The Los Alamitos Unified School District recognizes and supports advances in technology. While these technologies provide a valuable resource to the District, it is important that the District's use of technology be appropriate for District purposes. Inappropriate use may result in loss of employee productivity, service, compromised security, lost data, and other negative consequences.

District Regulation

District technology includes, but is not limited, to the District's Internet/Intranet/Extranet-related systems, email system, phone system including voice mail, video conferencing, 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 and 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. Public resources are appropriately used for District-related business;
 2. Applicable District policies and regulations, including those regarding harassment and nondiscrimination, are followed;
 3. 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. Passwords should not be stored in easily accessible areas, i.e., under keyboards, on monitors, or in desk drawers. Users shall not login others using their personal user ID or password credentials.
- C. The District reserves the right to periodically purge electronic mail messages stored on the District server.
- D. 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.
- E. 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 238 describing how students will be expected to use the equipment and what will constitute unacceptable behavior.
- F. Electronic mail use must be in accordance with guidelines established by the District. Electronic mail messages for broadcast to all employees must be approved by a District Administrator or a designee prior to being sent to the electronic mail account designated for this purpose. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.
- G. Employees will report all incidents of unacceptable use immediately without inquiry to their supervisor who will report it to the Assistant Superintendent of Human Resources and Instruction or Assistant Superintendent, Business Services, for handling. All incidents of viruses, malicious software or security failures shall be reported immediately to the IT Help Desk and the Assistant Superintendent, Business Services.

- H. All the rules of conduct described in the school's campus code and District's policies and regulations apply on the Internet and other on-line services. The user in whose name an on-line services account is issued is responsible for its proper use at all times. Users shall keep personal account numbers, home addresses, and telephone numbers private. They shall use the system only under their own account.
- I. 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.
- J. 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 configured to District standards.
- K. Prohibited uses of District technology include the following:
1. Using District technology for commercial advertising, gain, or fraud;
 2. Using District technology for unauthorized personal or non-profit purposes;
 3. Political activities;
 4. Religious activities;
 5. Intentionally disabling or bypassing security systems or procedures;
 6. Unauthorized use of another's passwords or computer to access files, resources or systems, or unauthorized use of an account belonging to another user;
 7. Unauthorized access to protected systems containing student, personnel, financial, or other data;
 8. Using District technology to access, obtain or distribute confidential, personal, or private information without authorization or unauthorized possession of any data that might be considered a violation of these rules in paper, magnet, or other form;
 9. Using District computers to copy software or using software in violation of copyright or license agreements;
 10. Copying District software, files or documents for personal use or downloading or installing personal software on District computers for non-District purposes;
 11. Unauthorized use or possession of services, real property, or intellectual property;
 12. 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. "Obscene material" is defined as (a) the subject as a whole appeals to the prurient interest (shameful or morbid interest in nudity, sex or excretion) of the average person, using contemporary community standards; (b) the work depicts or describes in a patently offensive way sexual conduct proscribed by the state statute, and (c) the work as a whole lacks serious literary, artistic, political, or scientific value;
 - 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.
 13. Forging documents or electronic mail messages or using District technology to create, send, or receive message using someone else's user name or address or portraying someone else as the originator of the message or document without authorization;
 14. Sending or forwarding chain letters which is defined as correspondence directing the recipient to send out multiple copies;
 15. 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;
 16. Using the network or electronic mail in a manner inconsistent with other District policies, regulations, or procedures;
 17. Intentionally disrupting network traffic or degrading or disrupting equipment and system performance;
 18. Accessing or exploring on-line locations, chat rooms such as "myspace", yahoo chat, etc., materials or on-line games that do not support the curriculum and/or appropriate for school-related work;
 19. Vandalizing and/or tampering with equipment, programs, files, system performance, or other components of the network, including copying, distributing, or modifying copyrighted software;
 20. Causing congestion on any technological system or interfering with the work of others, e.g., engaging in chain letters, unapproved chat rooms or in peer-to-peer networking applications such as Napster, Gnutella, etc., broadcasting messages to lists or individuals, modifying or deleting files;
 21. Attempting to infiltrate or "hack" into any technological system, or interfering with another person's ability to use that system, including password sniffing, using a keylogger, and/or port scanning;
 22. Using unauthorized fee-based services on the internet or via the phone system for dial-up connections;
 23. Intentionally wasting finite resources, e.g., on-line games, instant messaging;
 24. Coaching, helping, observing, or joining any unauthorized activity on any technological system;

25. Posting anonymous messages, unapproved web pages, or unlawful or libelous information on the system;
 26. Granting remote or local control of a networked system to a third party.
- L. Technology equipment (hardware or software) may not be taken, or copies to be taken, home or off-site without written permission signed by a District administrator.
 - M. 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.
 - N. Donated hardware and software must meet minimum standards and licensing requirements from the District IT department and must have board approval. 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 electronic mail;
 3. Disciplinary action, up to and including termination;
 4. Civil or criminal action against the offender, where appropriate.

Children's Internet Protection Act

1. In compliance with the Children's Internet Protection Act, the District is utilizing the Orange County Department of Education (OCDE)-installed filtering and/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 and configured by the OCDE. 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.
2. Students and staff may not disable the District's and/or OCDE'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.
3. 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.
4. 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 another person, or knowingly or recklessly post false or defamatory information about a person or organization.
5. 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 Web site - creates a likelihood of material disruption of the school's operations, students may face school discipline and criminal penalties.
6. Our District takes bullying and harassment by computer 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.
7. In the event of a claim that a student has violated this policy, the District will provide the student with notice of an opportunity to be heard in the manner set forth in the student handbook.

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:

- 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;
- Any costs, liabilities or damages caused by the way the user chooses to use network access;
- Any consequences of service interruptions or changes, even if these disruptions arise from circumstances under the control of the District;
- While the District supports the privacy of electronic mail, users must assume that this cannot be guaranteed.

Electronic Mail (E-mail)

1. All electronic mail messages, like all paper documents, are the property of the District and are subject to office policy, procedures, and control.
2. Electronic mail is for official office use only – not personal use. Electronic mail 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. As such, electronic mail messages become public documents available to the general public and subject to discovery in any legal proceedings.
3. The major purpose of electronic mail is informal communications; e.g., calendaring meetings, notes, reminders, phone messages, and simple questions or other similar purposes.

4. Electronic mail alone should not be used for any official communications (i.e., bulletins, letters.)
5. Electronic mail can be used to produce and distribute internal memoranda, as long as the sender ensures proper distribution (i.e., hard copies to staff without electronic mail capability, and delivery in a timely manner.)
6. Electronic mail messages should not contain profanity, racial or sexual slurs, or other unprofessional language.
7. Employees are responsible for keeping access to their electronic mail account secure and may be held accountable for any messages sent using their electronic mail account. Each user is expected to change their password on first use and every 90 calendar days thereafter and keep it secure. Continued use of a generic password, leaving a password where it can be found, giving the password to anyone other than their supervisor or leaving a computer unattended with electronic mail open can result in someone else sending messages in the owner's name. Automatic logging on to electronic mail without password entry for each use should not be used.
8. Unauthorized use, or forging, of email header information and creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type is prohibited.

Broadcast to All Electronic Mail Users

1. Prior to sending any message to all electronic mail users, the message must be reviewed by the appropriate principal or District Administrator as to its appropriateness. The initials of the approving person shall appear at the end of the announcement to show it has been approved.
2. Electronic mail shall not be used for mass circulation of announcements, minutes, event publicity, and other similar purposes to all District staff on the system without prior approval by the appropriate District Administrator. This includes sales, fund-raisers, or the birth or death announcements of non-employees and relatives of employees, unless approved in advance by the principal or District Administrator.
3. Inter-group announcements, such as birth, death, or marriage notices are to be used only within an individual school with prior approval of the principal. With the approval of the principal, they may be sent to other school principals, who will determine the distribution within their schools.
4. A specific address has been established for broadcast electronic mail. Approved messages are sent to this address. Network staff will broadcast only approved messages.

Districtwide Web Pages

1. Web pages and sites must adhere to the regulation described here. All sites and third-party consultants must also adhere to these policies.
2. All sites and consultants will adhere to Section 508 of American Disability Act and also follow the WC3 Web Content accessibility guidelines of the American Disability Act.
3. Los Alamitos Unified School District web pages will not include links to commercial sites that sell products and/or be sponsored from commercial companies in exchange for advertisement.
4. No illegal, threatening, offensive or harassing material or anything that can constitute a criminal offense will be permitted on the web pages. Any sensitive or questionable material will need approval from Superintendent or his/her designee.
5. The web pages will have a consistent look and feel and adhere to standards-based development viewable in common Internet browsers, i.e., Internet Explorer, Safari, Mozilla, etc.
6. Site Principals will be responsible for reviewing and approving site content as well as design consistency.
7. The Superintendent and his/her designee will have the right to remove websites or content that may be questionable, violate regulations, policies or state laws, or do not adhere to the standards mentioned in this document.

Virtual Private Network (VPN)

The purpose of this regulation is to provide the rule set for Remote Access IPSec or L2TP Virtual Private Network (VPN) connections to the Los Alamitos Unified School District educational network. This regulation applies to all Los Alamitos Unified School District employees, students, volunteers, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing VPNs to access the Los Alamitos Unified School District network. This regulation applies to implementations of VPN that are directed through an IPSec Concentrator.

Approved Los Alamitos Unified School District employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of VPNs, which are a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees. Further details may be found in the *Remote Access Regulation*. In addition:

1. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to Los Alamitos Unified School District internal networks.
2. VPN use is to be controlled using either a one-time password authentication such as a token device or a public/private key system with a strong passphrase.
3. When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.
4. Dual (split) tunneling is NOT permitted; only one network connection is allowed.
5. VPN gateways will be set up and managed by Los Alamitos Unified School District IT department.
6. All computers connected to Los Alamitos Unified School District internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard (provide URL to this software); this includes personal computers.

7. VPN users will be automatically disconnected from Los Alamitos Unified School District's network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
8. The VPN concentrator is limited to an absolute connection time of 24 hours.
9. Users of computers that are not Los Alamitos Unified School District-owned equipment must configure the equipment to comply with Los Alamitos Unified School District's VPN and Network regulations.
10. Only Los Alamitos Unified School District approved VPN clients may be used.
11. Los Alamitos Unified School District employees and third parties will ensure that the device attaching to the VPN is free from virus and malicious code to protect the Los Alamitos Unified School District network.
12. By using VPN technology with personal equipment which is not supported or recommended, users must understand that their machines are a de facto extension of Los Alamitos Unified School District's network, and as such are subject to the same rules and regulations that apply to Los Alamitos Unified School District-owned equipment, i.e., their machines must be configured to comply with board approved AUP (Acceptable Use Policy) and Security Policies.

Any employee found to have violated this regulation may be subject to disciplinary action, up to and including termination of employment. Students will be subject to student disciplinary action based on districts student code of conduct. Any violation from third party (volunteers, consultants, etc.) entities will be subject to legal and monetary compensation.

<u>Term</u>	<u>Definition</u>
IPSec Concentrator	A device in which VPN connections are terminated.
VPN	Virtual Private Network allowing access to internal district resources for business purposes.
ISP	Internet Service Provider providing Internet/Intranet access to district and school sites.

Remote Access

The purpose of this regulation is to define standards for connecting to Los Alamitos Unified School District's network from any host. These standards are designed to minimize the potential exposure to Los Alamitos Unified School District from damages which may result from unauthorized use of Los Alamitos Unified School District resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical Los Alamitos Unified School District internal systems, etc.

This regulation applies to all Los Alamitos Unified School District employees, students, volunteers, contractors, vendors and agents with a Los Alamitos Unified School District-owned or personally-owned computer or workstation used to connect to the Los Alamitos Unified School District network. This regulation applies to remote access connections used to do work on behalf of Los Alamitos Unified School District, including reading or sending email and viewing intranet web resources.

Remote access implementations that are covered by this regulation include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems, etc.

1. It is the responsibility of Los Alamitos Unified School District employees, contractors, vendors and agents with remote access privileges to Los Alamitos Unified School District's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Los Alamitos Unified School District.
2. General access to the Internet for recreational use by immediate household members through the Los Alamitos Unified School District Network on personal computers is permitted for employees that have flat-rate services. The Los Alamitos Unified School District employee is responsible to ensure the family member does not violate any Los Alamitos Unified School District policies or regulations, does not perform illegal activities, and does not use the access for outside business interests. The Los Alamitos Unified School District employee bears responsibility for the consequences should access be misused.
3. Please review the following regulations for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of Los Alamitos Unified School District's network:
 - a. *Virtual Private Network (VPN) Policy*
 - b. *Acceptable Use Policy*

Requirements

1. Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases.
2. At no time should any Los Alamitos Unified School District employee provide their login or email password to anyone, not even family members.
3. Los Alamitos Unified School District employees and contractors with remote access privileges must ensure that their Los Alamitos Unified School District-owned or personal computer or workstation, which is remotely connected to Los Alamitos Unified School District's corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
4. Los Alamitos Unified School District employees and contractors with remote access privileges to Los Alamitos Unified School District's corporate network must not use non-Los Alamitos Unified School District email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct Los Alamitos Unified School District business, thereby ensuring that official business is never confused with personal business.
5. Routers for dedicated ISDN lines configured for access to the Los Alamitos Unified School District network must meet minimum authentication requirements of CHAP.
6. Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
7. Frame Relay must meet minimum authentication requirements of DLCI standards.
8. Non-standard hardware configurations must be approved by Director of Technology and the Assistant Superintendent and must meet minimum security configurations for access to hardware.
9. All hosts that are connected to Los Alamitos Unified School District internal networks via remote access technologies must use the most up-to-date anti-virus software (place url to corporate software site here), this includes personal computers.

10. Personal equipment that is used to connect to Los Alamitos Unified School District's networks must meet the requirements of Los Alamitos Unified School District-owned equipment for remote access.
11. Organizations or individuals who wish to implement non-standard Remote Access solutions to the Los Alamitos Unified School District production network must obtain prior approval from Director of Technology and the Assistant Superintendent.

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Students will be subject to student disciplinary action based on districts student code of conduct. Any violation from third party (volunteers, consultants, etc.) entities will be subject to legal and monetary compensation.

<u>Term</u>	<u>Definition</u>
Cable Modem	Cable companies such as AT&T Broadband provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet at over 1.5 Mbps. Cable is currently available only in certain communities.
DSL	Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet).
Remote Access	Any access to Los Alamitos Unified School District's corporate network through a non-Los Alamitos Unified School District controlled network, device, or medium.

~ PLEASE KEEP PAGES 2-7 FOR YOUR RECORDS ~