

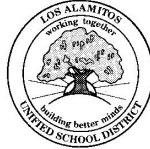
Print Name: \_\_\_\_\_  
*Student to PRINT - Last name, First name*

Signature: \_\_\_\_\_  
*Student Signature*

Date: \_\_\_\_\_

Month/Year of Graduation: \_\_\_\_\_  
*(not applicable to K-8)*

***MUST BE TURNED IN AT REGISTRATION***



**Los Alamitos Unified School District  
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" 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

We are pleased to announce that electronic information services are available to students 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 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 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 Regulation

District technology includes, but is not limited, to the District's Internet/Intranet/Extranet-related systems, email system, phone system including voice mail, cell phones, MP3 player, iPods, wireless communication, 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. 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 238 describing how students will be expected to use the equipment and what will constitute unacceptable behavior.
- E. Electronic mail use must be in accordance with guidelines established by the District. Use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.
- F. 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.
- G. 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 personal blogging, instant messaging, on-line shopping, video streaming, video downloads, or gaming is not allowed.
- H. 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.

- I. 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.
- J. 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;
    - 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.
  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.
- K. 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.
- L. 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.
- M. 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. You should not delete this information unless instructed to do so by a staff member.
- N. 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.
- O. Using District Technology, you will not: disclose your personal contact information or disclose other people’s personal contact information. You are encouraged to follow this rule in your use of Personal Technology as well. Again, if your use of Personal Technology causes disruption to the school community, you may be disciplined.
- P. 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.
- Q. 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.
  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 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.

- B. 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.
- 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 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 Web site - creates a likelihood of material disruption of the school's operations, students may face school discipline and criminal penalties.

#### Cyberbullying and Sexting

- 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.
- C. Cyberbullying includes posting or sharing private information about another person that is private.
- D. Cyberbullying includes 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 MySpace or Facebook profiles.
- E. Cyberbullying includes posting or sharing photographs of other people without their permission.
- F. 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.
- G. 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.
- H. All students or others who experience, witness or become aware of Cyberbullying shall immediately report it to a teacher or District administrator.
- I. You may not send, share, view or possess pictures, text message, e-mails or other material of an obscene nature in electronic or any other form on Personal Technology at school or school-related activities, or using District Technology.

#### 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) 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.
- B. 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.
- C. The major purpose of electronic mail is informal communications; e.g., calendaring meetings, notes, reminders, phone messages, and simple questions or other similar purposes.
- D. Electronic mail alone should not be used for any official communications (i.e., bulletins, letters.)
- E. 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.)
- F. Electronic mail messages should not contain profanity, racial or sexual slurs, or other unprofessional language.
- G. Unauthorized use, or forging, of email header information and creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type is prohibited.

**~ PLEASE KEEP PAGES 2-6 FOR YOUR RECORDS ~**