

**San Jacinto Unified School District
Technology Acceptable Use Agreement**

TERMS AND CONDITIONS

Please read the following carefully before signing this document.

Internet access is coordinated through a complex association of government agencies, and regional and state networks. In addition, the smooth operation of these networks relies upon the proper conduct of the end users who must adhere to strict guidelines. These guidelines are provided here so that you are aware of the responsibilities you are about to receive.

In general this requires efficient, ethical and legal utilization of the network resources. If a user violates any of these provisions, his or her account will be terminated and future access could possibly be denied. The signature(s) at the end of this document is (are) legally binding and indicates the party (parties) who signed has (have) read the terms and conditions carefully and understand(s) their significance. It is the responsibility of all San Jacinto Unified School District (SJUSD) employees, students, and others who use or access SJUSD's technological resources to understand and follow this Technology Acceptable Use Policy (AUP).

All access to Internet sites are routed through a "technology protection measure" designed to filter out material that is in violation of the District Internet policies. This filter will block most objectionable material, but users must be aware that the filter may miss some objectionable material and these sites should be reported immediately for review. A review process is available to block sites with objectionable material. There is also a review process to request the unblocking of sites that users believe contain material that has educational benefit.

Definitions

- System/Network shall mean the technology services and equipment owned and/or provided by San Jacinto Unified School District (SJUSD) for the use of SJUSD School employees, students, and other authorized users, including but not limited to: computers/tablets, Internet, telephones, fax machines, voice mail, email, electronic pagers, cell phones, and radios.
- Access to the Internet – An electronic device shall be considered to have access to the Internet if such device is equipped with a network port, wireless card, Wi-Fi or is connected to a computer network, which has access to the Internet.
- Minor/Student shall mean an individual who has not attained the age of 18.
- Obscene shall have the meaning given such term in section 1460 of title 18, United States Code.
- Child pornography shall have the meaning given such term in Section 2256 of title 18, United States Code.
- Harmful to minors shall mean any picture, image, graphic image file, or other visual depiction that:
 - Taken as a whole and with respect to minors, appeal to a prurient interest in nudity, sex, or excretion;
 - Depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and
 - Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.
- Hacking shall mean attempting to gain unauthorized access to computer and network system connected to the Internet.
- Gaming shall mean the practice of gambling including the playing of games that simulate gambling whether or not the gaming involves a monetary transaction.
- Technology protection measure shall refer to a proxy server that blocks and/or filters Internet access.
- Authorized employee/student as used herein shall refer to an adult staff member, volunteer, or student of San Jacinto Unified School District.

1. **Acceptable Use** - The network is provided for employee/student use to conduct research and communicate with others on academic topics and to engage in legitimate District business. Individual users of the district computer networks are responsible for their behavior and communications on those networks. It is presumed that users will comply with District standards and will abide by the policies specified herein. Violations of the District's policy described will result in access privileges suspended or revoked as well as other disciplinary action as warranted. Any commercial, political, or unauthorized use of those materials or services, in any form, is forbidden. All copyright laws must be observed.
2. **Unacceptable Use** - Transmission of any material in violation of any U.S. or state statute or regulation is prohibited. This includes, but is not limited to: copyright infringement, threatening or obscene material, or inappropriate use of material protected by trade secret or illegal gaming. Use for commercial activities is not acceptable. Use for product advertisement or political lobbying is also prohibited. Any transmission or reception of pornographic material is expressly prohibited.

Employees/Students are responsible for following generally accepted social standards for use of a publicly owned and operated communication tool. Employees/Students will maintain high standards of ethical conduct while using the system. Examples of unethical, unacceptable use of District technology equipment include the following:

- Sending, displaying, or accessing pornographic, abusive, obscene, or other objectionable language, graphics, or other media
- Unauthorized disclosure, use, and dissemination of personal information about students or employees
- "Hacking" or otherwise engaging in unlawful activities while online
- Using obscene language
- Cyber-bullying
 - **Flaming** – Online fights using electronic messages with angry and vulgar messages
 - **Harassment** – Repeatedly sending nasty, mean and insulting messages
 - **Sexting** - is the act of sending sexually explicit messages or photos electronically, primarily between mobile phones.
 - **Denigration** – "Dissing" someone online, Sending or posting rumors to damage a person's reputation
 - **Impersonation** – Pretending to be someone else and sending material to get that person in trouble
 - **Outing** – Sharing someone's secrets or embarrassing information or pictures online
 - **Exclusion** – Intentionally and cruelly excluding someone from an online group
 - **Cyberstalking** – Repeated, intense harassment that includes threats and creates fear
- Harassing, insulting, or attacking others
- Intentionally damaging computers, computer systems, data, files, information or computer networks
- Violating copyright laws
- Using or distributing another's password
- Trespassing in another's folders, work, or files
- Intentionally wasting limited resources
- Employing the network for outside business or commercial purposes
- Sending or receiving unethical, illegal, immoral, inappropriate, or unacceptable information of any type
- Engaging in activities that cause disruption to the network or its systems
- Attempting to bypass system security measures
- Reposting or forwarding a message that was sent to you privately without permission of the person who sent you the message
- Posting chain letters or engaging in "spamming" - i.e. sending an annoying or otherwise unnecessary message to a large number of people
- Any other activities not appropriate in an educational forum

3. **Privileges** – Use of the District’s network is a privilege, and unacceptable use will result in a cancellation of those privileges. The Director of Technology, in collaboration with district/school administration may close an account at any time as required for inappropriate use. District/school administration may request the Director of Technology to deny, revoke, or suspend specific user accounts. The violation of any item contained in this policy may result in the loss of computer/tablet access and/or other disciplinary action, as well as possible punitive action as provided for by local, state, and federal law.
4. **Network etiquette** - *You are expected to abide by the generally accepted rules of network etiquette. These include (but are not limited to) the following:*
 - *Be polite.*
 - *Use appropriate language.*
 - *Do not reveal your personal address or phone numbers of students or colleagues.*
 - *Electronic mail (e-mail) is not guaranteed to be private. **Messages relating to or in support of illegal activities must be reported to the Director of Technology or District/School administration.***
 - *All communications and information accessible via the network should be assumed to be San Jacinto Unified School District private property.*
5. **Network Use Disclaimer** - San Jacinto Unified School District makes no guarantees of any kind, whether expressed or implied, for the service it is providing. San Jacinto Unified School District will not be responsible for any damages you suffer. This includes loss of data resulting from delays, non-deliveries, incorrect delivery, or service interruptions caused by its own negligence or your errors or omissions. Use of any information obtained via the District’s network is at your own risk.
6. **Security** - Security on any computer system is a high priority, especially any system that has many users and/or Internet access. Employees/students shall not let others use his or her account or password, as he or she is responsible for all actions related to his or her account. Employees/students must notify school administrators immediately if their password is lost or stolen or if they think someone has access to their account. Students are to use only the network directories and resources that have been assigned for their use. Unauthorized access to any other level of the system, or other system resource, is strictly prohibited. Users will make no attempt to bypass the district anti-virus software, firewall, filtering, and/or safeguards. When finished with a computer, the student is expected to logout where appropriate. If you can identify a security problem on the District’s network, notify Technology Services at 951-929-7700 ext. 4500. Do not use another individual's account. Attempts to login to the District’s network or any district computer as a system administrator will result in suspension or cancellation of user privileges.
7. **Vandalism** - Vandalism will result in cancellation of privileges. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the District’s network, or any of the above listed agencies or other networks that are connected to the District’s network. This includes, but is not limited to, the uploading or creation of computer viruses, destroying and/or defacing any technology equipment.
8. **Access to Internet and Other Technologies by Adults/Students** - Adults/Students accessing the System/Network when working as an employee/student or volunteer of San Jacinto Unified School District; when attending trainings, meetings, conferences, or other events sponsored by SJUSD or at a facility of which SJUSD has otherwise been granted permission of use shall be subject to the rules and regulations specified in the Acceptable Use Policy and the Child Internet Protection Act.
 - The employee/student whose name an on-line account is issued is responsible for its proper use at all times. Employees/student shall keep account information, home addresses and telephone numbers private. They shall use the System only under their own account number.
 - Employees/students shall use the system primarily for purposes related to their employment/education within the County. Commercial use of the system is strictly prohibited.

- Any illegal use of San Jacinto Unified School District's network systems, or use in support of illegal activities is prohibited. Illegal use includes use that violates local, state and/or federal law. This includes, but is not limited to, the following: stalking others, transmitting or originating any unlawful, fraudulent or defamatory communications, transmitting copyrighted material beyond the scope of fair use without permission of the copyright owner, or any communications where the message or its transmission of distribution, would constitute or would encourage conduct that is a criminal offense. Users shall not use any technology or system to promote unethical practices or any activity prohibited by law or district policy.
- Activities that interfere with or disrupt network users, services, or equipment are prohibited. Such interference or disruption includes, but is not limited to, distribution of unsolicited advertising or mass mailings, "spamming," propagation of computer worms or viruses; and using district, county systems or the K12 High Speed Network to make or attempt to make unauthorized entry to other computational, informational or communications devices or resources. For the purpose of this AUP, "unsolicited advertising" includes any transmission that describes goods, products, or services for sale.
- Employees/students shall not transmit material that is threatening, obscene, disruptive or sexually explicit, or 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, or otherwise inappropriate for training or school/work-related uses.
- Employees/students shall not engage in any type of gaming activities on the system.
- Adult users shall not download or install any games on District-owned devices other than those used specifically for educational purposes. All downloads/installs shall be approved by administration.
- Student users may engage in the playing of computer games during non-instructional time.
- Users shall not use the system to engage in unauthorized hacking or attempts to otherwise compromise any computer or network system's security. Unauthorized review, duplication, dissemination, removal, damage or alteration of files, passwords, computer systems or programs, voicemail messages or other property of SJUSD or improper use of information obtained by unauthorized means, may be grounds for disciplinary action.
- Users shall not connect any equipment to the system/network without prior approval from Technology Services. An individual will not move equipment unless Technology Services in collaboration with school/district administration has given permission.
- Copyrighted material may not be placed on the system without the author's permission. Users may download copyrighted material for their own use only in accordance with copyright laws.
- Users shall not read other users' electronic mail or files; they shall not attempt to interfere with other users' ability to send or receive electronic mail nor shall they attempt to read, delete, copy, or modify other users' mail without authorization. Users shall not forge other users' mail.
- Users are encouraged to keep messages brief. Use of the e-mail system is permitted so long as that use is appropriate, does not violate any other district or county policies, and is acceptable to the individual employee's supervisor or student's teacher/administrator.
- The following practices are prohibited:
 - Sending or relaying chain letters.
 - Sending unsolicited jokes or similar material.
 - Use in support of partisan political activities.

- Use for private or personal activities that exceed San Jacinto Unified School District's related research, instruction, or administrative applications.
 - Visiting pornographic, racist or otherwise objectionable web sites.
 - Any other use that is unacceptable or not in keeping with the role, mission or goals of San Jacinto Unified School District as determined by District/School Administration.
- Users shall report any security problem or misuse of the system to the Director of Technology, School Administration, or designee.
 - Adult users shall not load or download from the Internet any software on San Jacinto Unified School District equipment without prior authorization from Technology Services. This includes media players, screen savers, wallpapers, games, widgets, etc....
 - Student users may download material to their devices as long as the material meets the requirements listed in this AUP. Any material deemed to be offensive, distracting to the educational environment, sexually explicit, racist, or demeaning will be cause for confiscation of the device and appropriate disciplinary action.
9. **Access to Internet by Minors/Students** - Minors/Students accessing the system/network when working as an employee, student, and/or volunteer of SJUSD; when attending trainings, meetings, conferences, or other events sponsored by San Jacinto Unified School District or at a facility of which San Jacinto Unified School District has otherwise been granted permission of use shall be subject to the rules and regulations as adult users. In accordance with the **Child Internet Protection Act**, minors shall be subject to the following rules:
- Minors shall not access material that is obscene, pornographic, harmful to minors, or otherwise inappropriate for educational or work-related uses
 - Minors shall only use electronic mail, chat rooms and other forms of direct electronic communications for purpose related to education within the context of a school-related assignment activity or for purposes related to work, including volunteer, at San Jacinto Unified School District.
 - Minors shall not disclose personal identification information of any kind on the Internet.
10. **Privacy** - Employees/Students have no right to privacy as to any information or file transmitted or stored through the system, including the San Jacinto Unified School District computer systems, voicemail, text messaging, electronic mail or other technical resources. San Jacinto Unified School District reserves the right to retrieve and read any message or file. All users should be aware that when a message is deleted, it may still be possible to recreate the message; therefore, ultimate privacy of messages cannot be guaranteed to anyone. The reliability of passwords for maintaining confidentiality cannot be guaranteed.
11. **“Apps” Ownership** – the purchase of iPads and any associated applications (apps) will be approved by District administration making the purchase. The purchase of the devices and apps will be through the regular requisition process. Once the requisition has cleared the approval process, the designated volume purchaser(s) shall obtain the apps and notify the end user(s) once redemption codes are issued. The downloading of District purchased apps to personal devices or personal account IDs is prohibited and may constitute a gift of public funds. All District purchased apps will be installed using District created IDs.
12. **Policy Violation** - Any violation of this policy and regulation may result in the loss of access to the system, or any component part by San Jacinto Unified School District, and may be referred to applicable law enforcement agencies when necessary. Any violation of this policy by a San Jacinto Unified School District employee/student may also be grounds for disciplinary action.

13. Public Records and Retention:

- Information stored on the system or San Jacinto Unified School District equipment, including e-mail, e-mail attachments, web postings, and voice mail messages may become records of San Jacinto Unified School District. San Jacinto Unified School District records pertaining to SJUSD's business, whether paper or computerized are considered public records and, therefore, may be subject to disclosure under the Public Records Act ("PRA") and Title 5, section 16020, et seq., of the California Code of Regulations, pertaining to the retention and destruction of school records.
- A San Jacinto Unified School District e-mail account is not intended for permanent storage of e-mail. San Jacinto Unified School District may retain or dispose of an employee's e-mail, whether an employee is currently or formerly employed by San Jacinto Unified School District. E-mail account inboxes and outboxes may be purged as often as every 90 days by San Jacinto Unified School District.

I understand and will abide by the above Terms and Conditions for Technology Acceptable Use Agreement. I further understand that any violation of the regulations above is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked; school disciplinary action may be taken and/or appropriate legal action.

Approved: _____

SAN JACINTO UNIFIED SCHOOL DISTRICT
San Jacinto, California

Revised: 5/14/13