San Jacinto Valley Academy (SJVA)

Board Policy – Acceptable Use and Internet Safety Policy BP 6162.7

The Internet is an educational resource connecting millions of computers and computer users from all over the world. Use of the Internet for educational projects will assist in preparing success in life and work in the 21st Century. Educators agree it is important that students are well informed of the Internet's capabilities, as well as how to use it responsibly. The San Jacinto Valley Academy recognizes the need to safeguard our students, while enriching our core curriculum.

A. General Principles of Access

1. The San Jacinto Valley Academy ("SJVA") provides access to the Internet, including access to e-mail, for its employees, staff members, students, and guests. Guests include but are not limited to parents, substitute teachers, temporary school employees, parent volunteers, and other school volunteers.
2. Internet access and the use of e-mail through the use of the School's system, has an intended educational purpose. The term "educational purpose" includes use of the system by students and their parents for learning activities, employee professional or career development, communication between teachers, students and their parents and the facilitation of information-sharing between teachers and administrators. If any user has a question whether their Internet use is consistent with the School's educational purpose, goals, and mission, s/he should consult with the appropriate supervisor, principal, teacher, etc.
3. This Internet Acceptable Use Policy governs all electronic activity, including e-mail and access to the Internet, which is undertaken by employees, students, and parents/guardians either in their official school duties or as part of the educational, instructional or extracurricular programs connected to the school. No school employee, student, or parent/guardian may engage in activities prohibited by this Internet Acceptable Use Policy, whether through the School's Internet service or through another Internet Service Provider, when those activities are undertaken either in their official school duties or as part of the educational, instructional, or extracurricular programs.
4. SJVA reserves the right to terminate any user's access to the Internet, including access to e-mail, at any time and for any reason. SJVA reserves the right to monitor all Internet access, including all e-mail, through use of the School's system. SJVA specifically reserves the right to revoke access and/or take other appropriate disciplinary action, with respect to any user who violates this policy.

B. Internet Safety

1. It is the policy of the San Jacinto Valley Academy to protect students from inappropriate material on the Internet, as well as to ensure the safety and security of students when using electronic communications such as electronic mail. This is done both through proper adult supervision of all students using the Internet and by "Technology Protection Measures" such as content filtering, which will restrict minors' access to materials deemed "harmful to minors" including pornography, violence and "hate" sites. Such filtering may only be removed for teachers and students for bona fide research or

other lawful purposes with permission from and administrator or his or her designee. Any use of instant messaging and chat rooms is prohibited except for educational purposes. Violations may result in cancellation of Internet privileges and disciplinary and possible legal consequences.

2. Harassment of all types against students or staff, with a particular focus on “Cyberbullying” will not be tolerated. "Cyberbullying" includes the posting of harassing messages, direct threats, social cruelty, or other harmful text or images on the Internet, social networking sites, or other digital technologies, as well as breaking into another person's account and assuming that person's identity in order to damage that person's reputation or friendships.

3. SJVA’s response to harassment and/or “Cyberbullying” is to prevent bullying by establishing a positive, collaborative school climate and clear rules for student conduct. The school may provide students instruction in the classroom or other school settings that promotes communication, social skills, and assertiveness skills and may involve parents/guardians, staff, and community members in the development of strategies to prevent and respond to bullying. Students shall be taught the skills necessary to reduce violence, including communication skills, anger management, bias reduction and mediation skills.

4. Unauthorized disclosure, use and dissemination of personal information regarding minors or other users are prohibited.

C. School Limitation of Liability

1. The School makes no warranties of any kind, either express or implied, that the functions or the services provided by or through the School system will be error-free or without defect. The School will not be responsible for any damage users may suffer, including but not limited to, loss of data or interruptions of service. The School is not responsible for the accuracy or quality of the information obtained through or stored on the system. The School will not be responsible for financial obligations arising through the unauthorized use of the system.

D. Due Process

1. SJVA will cooperate fully with local, state, or federal officials in any investigation concerning to or relating to any illegal activities conducted through the School system or through any School user accounts.

2. In the event there is an allegation that a student has violated the Acceptable Use Policy, the parent will be provided with an oral and/or written notice of the alleged violation and an opportunity to present an explanation. This is in accordance with the due process rights of students.

3. Employee violations of the Acceptable Use Policy will be handled in accordance with due process rights, School policy, and California State Education Law.

E. Privacy

1. System users shall be made aware that they have no expectation or right of privacy in the contents of their personal files on the School system since the system will be monitored by a system operator(s).

F. Copyright Infringement and Plagiarism

1. Users will not plagiarize works that they find on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were original to the user.
2. Users will respect the rights of copyright owners and not infringe on those rights. Copyright infringement occurs when an individual inappropriately reproduces a work that is protected by a copyright. If a work contains language that specifies acceptable use of that work, the user should follow the expressed requirements. If the user is unsure whether or not they can use a work, they should request permission from the copyright owner.

G. Acceptable Use Policy

The following guidelines are to be applied when using the School system:

1. Threats to personal safety of students

a. Users will not post personal contact information about themselves or other people (i.e. address, telephone, school address, work address, etc.).
b. Users will not agree to meet with someone they have met on-line without their parents or guardian's approval and participation.
c. Users will promptly disclose to their teacher or other school employee any message they receive that is inappropriate or makes them feel uncomfortable.

2. Illegal Activities

a. Users will not commit vandalism or engage in hacking activities. Vandalism or hacking will result in cancellation of system use privileges as well as possible prosecution. Vandalism is defined as any malicious attempt to harm or destroy property, data of another user, the internet, or any other networks that are connected to the internet. This includes, but is not limited to, the intentional uploading or creation of computer viruses, attempts at gaining unauthorized access, or changing on-line materials without permission. Tampering with or misuse of the computer system, hacking, or taking any other action inconsistent with this protocol and regulation will be viewed as a security violation. Violators will be responsible for any financial damages caused by their actions.
b. Users will not attempt to gain unauthorized access to the School system or to any other computer system beyond their authorized access.
c. Users may not possess pirated software. Pirated software means any software, which has been downloaded or copied illegally, or is otherwise in the user's possession, without the appropriate registration of the software, including the payment of any fees owed to the owner of the software.
d. Users may not download or otherwise add software programs to the School system without permission from the administration.
e. Users shall not use the School system or Internet to access, transmit or retransmit material which promotes violence or advocates destruction of property, including information concerning the manufacture of destructive devices, such as explosives, fireworks, smoke bombs, incendiary devices or the like.
f. Users shall not use the School system or Internet to access, transmit or retransmit material which advocates or promotes hatred against particular individuals or groups of individuals or advocates or promotes the superiority or inferiority of one racial, ethnic or religious group.

g. Users will not use the School system to engage in any illegal act.

3. System Security

a. Users may not utilize the network in such a way that it will disrupt the use of the network by others.
b. Staff and students are responsible for the accounts for which they have been provided passwords. Passwords should not be shared.
c. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the Internet and/or to the School's computer system.
d. Users will immediately notify a teacher or administrator if they have identified a possible security problem. Users will not go looking for security problems, because this may be construed as an illegal attempt to gain access.
e. Users will avoid the inadvertent spread of computer viruses by following the School virus protection procedures if they download files onto the School's computers and/or networks.

4. Inappropriate Language

a. Restrictions against inappropriate language apply to all forms of communication using the School's network or internet connection.
b. Users will not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language.
c. Users will not post information that, if acted upon, could cause damage or a danger of disruption to the Schools electronic systems.
d. Users will not engage in personal attacks, including prejudicial or discriminatory attacks.
e. Users will not harass another person. If a user is told by a person to stop sending those messages, they must stop.
f. Users will not knowingly or recklessly post false or defamatory information about a person or organization.

5. Respect for Privacy

a. Users will not repost a message that was sent to them privately without permission of the person who sent them the message.
b. Users will not post private or identifying information about any minor, other person, or themselves.

6. Respecting Resource Limits

a. Users will not download files larger than 50 megabytes without permission.
b. Users will not post chain letters or engage in "spamming".
c. Access to news groups, if granted, will be limited to acceptable discussions.

7. Inappropriate Access to Material

a. Users will not use the School system to access material that is considered profane or obscene (pornography), that advocates illegal acts, or that advocates violence or discrimination towards other people (hate literature). School employees may access the above material only in the context of legitimate research.

b. If a user inadvertently accesses such information, they should immediately disclose the inadvertent access to a school administrator or other appropriate school employee. This will protect users against an allegation that they have intentionally violated the Acceptable Use and Internet Safety Policy.

8. Privileges

a. The use of the Internet and the School system by students and staff is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges and disciplinary and possible legal consequences.

H. Electronic Mail Policy

These guidelines are intended to help you make the best use of the electronic mail facilities at your disposal. You should understand the following:

The San Jacinto Valley Academy provides electronic mail to staff to enable them to communicate effectively and efficiently with other members of staff and other companies or organizations related to job responsibilities. SJVA reserves the right to monitor all electronic mail communications. When using the SJVA electronic mail facilities you should comply with the following guidelines. Any breach of the SJVA Electronic Mail Policy may lead to disciplinary action.

Guidelines:

1. Check your electronic mail daily to see if you have any messages.
2. Include a meaningful subject line in your message.
3. Delete electronic mail messages when they are no longer required.
4. You must respect the legal protections to data and software provided by copyright and licenses.
5. Do not forward electronic mail messages sent to you personally to others, particularly newsgroups or mailing lists, without the permission of the originator.
6. Do not use electronic mail for personal reasons.
7. Do not send excessively large electronic mail messages or attachments.
8. Do not send unnecessary messages such as festive greetings, jokes, or other non-work items by electronic mail.
9. Do not participate in chain or pyramid messages or similar schemes.
10. Do not represent yourself as another person.
11. Do not use electronic mail to send or forward material that could be construed as confidential, illegal, political, obscene, defamatory, threatening, offensive, or libelous.

I. Chromebooks

SJVA purchased Google Chromebooks for student use throughout the school. The teacher in each of these rooms is responsible for the care and security of these Chromebooks. Below are the guidelines for the care and protection of the teacher assigned Chromebooks.

1. Students are not allowed to stream any kind of audio/video under your supervision.
2. Students are not allowed to change any settings on the device assigned to them.

3. If a Chromebook breaks or needs technical assistance please go to help desk and fill out a help ticket describing the problem.
4. Always monitor the students don’t leave them unattended with the devices.
5. Report to IT department immediately in case:

- You find someone using in appropriate website
- You find a broken Chromebook
- The locks were left unlocked or are missing

6. Make sure to check both the locks on the cart before leaving the campus. If you leave the room with the cart unlocked, make sure the room is locked.

BP 6162.7
Revised: July 16, 2015

Acceptable Use and Internet Safety Policy Agreement

I have read the San Jacinto Valley Acceptable Use and Internet Safety Policy and agree to abide by the rules and policies stated in this document.

Name (please print legibly) ____

I am a □ Student □ Employee

Signature ____

****

Parent Name (if above is student) _______________________________________

Parent Signature ____