

SERVITE HIGH SCHOOL TECHNOLOGY



STUDENT ACCEPTABLE USE POLICY

Revised 8/19/2010

Table of Contents

Section

200) Purpose

201) Definitions

- a) SHS Network Related Technologies (“SHS Network”)
- b) Electronic Mail (“E-mail”)
- c) Internet
- d) Personal Electronic Devices
- e) Password
- f) Students
- g) Website

202) General Provisions

- a) Responsibilities of Servite High School
- b) Students
- c) Parents and Guardians
- d) Disclaimer

203) Terms and Conditions

- a) Acceptable Use
- b) Unacceptable use
- c) Security
- d) Privileges and Rights
 - i) Privacy
 - ii) Access
 - iii) Safety

204) Enforcement

- a) Filtering
- b) Monitoring

205) Assumption of Risk

206) Indemnification

207) Sanctions

200) Student Computer Disciplinary Code (SCDC)

201) Accessing Inappropriate Material

202) Improper Network Access

203) Game-play and Messaging

204) Compromising the integrity of credentials

205) Irresponsible Use of Technology Hardware

206) Violating Academic Integrity

100 PURPOSE

The purpose of the Acceptable Use Policy (“AUP”) is to set forth standards governing Servite High School (“SHS”) students’ use of the SHS Network Related Technologies (“SHS Network”). This policy promotes the ethical, legal, and educational use of the SHS Network. Personal electronic devices will be governed under this policy when such devices are attached to the SHS Network. This policy is complementary to and does not replace any policies regarding electronic communications in the student handbook.

This policy also sets forth the rules under which students may continue their access and use of these resources. Student use of information resources must be consistent with the educational purposes for which these resources have been provided. Use of the SHS network is a privilege that is provided to help students complete and deliver educational objectives. The SHS Network provides students with the means for communicating effectively with teachers, administrators, other schools, the public and each other. These resources should be used in a manner that both enhances students’ educational experiences and complies with this policy and regulations already established by the SHS Administration.

101 DEFINITIONS

- A. SHS Network Related Technologies (“SHS Network”)**
The SHS Network is the system of interconnected computers, servers, routers, switches, hubs, wireless access points, databases, services, and various software packages. These components may function through established wired or wireless connections and work together to allow access to a wide variety of resources including but not limited to: e-mail, the internet, curriculum guides, textbooks, presentations, videos, music, and research materials.
- B. Electronic Mail (“E-Mail”)**
Electronic Mail includes all electronically transmitted information, including any combination of text, graphics, audio, video, or other information created on or received by a computer system and includes the transmission data, message text, and all attachments.
- C. Internet**
The internet is a global network made up of many smaller contributing networks. Its services are intended to support the open exchange of information among a large and diverse population of connected institutions.
- D. Personal Electronic Devices**
Personal electronic devices include, but are not limited to, cellular telecommunication devices such as cellular phones, pagers, media players, storage devices and personal digital assistants that may or may not be physically connected to the network infrastructure.
- E. Password**
A Password is a secret word or a combination of letters and numbers that must be used to gain access to protected content, such as the SHS Network, an online service, or certain software.

F. Students

Students are young men whose current status is active and enrolled in classes at Servite High School

G. Website

A Website is a collection of ‘pages’ or files on the Internet that are linked together and managed by a company, institution, or individual.

102 GENERAL PROVISIONS

A. Responsibilities of Servite High School

The SHS Faculty and Staff are responsible for facilitating students in the pursuit of education-related SHS Network use. They will actively monitor and engage students while using the internet and the SHS Network. Faculty and staff members will also demonstrate and encourage responsible computer and internet use while connected to the SHS Network.

The SHS Technology Department will provide a network that is reliable and functional. The SHS Administration reserves the right to revise this Acceptable Use Policy as it deems necessary. The Administration will post the current policy on the SHS Website and will provide notice via the website and/or e-mail to users of any revisions. Students and parents are encouraged to read this policy regularly and thoroughly.

B. Responsibilities of Student

All students shall adhere to the provisions of this document as a condition of their continued use of the SHS Network. This policy is enabled anytime the student is on the SHS Campus, there is a connection to the SHS Network through hardwired or wireless connections, or through external connections including but not limited to the external SHS website and VPN connections.

C. Responsibilities of Parent/Guardian

The parents/guardians of a student are responsible for encouraging and supporting the use of technology and for learning and monitoring the standards of behavior their student(s) should follow when using any media or online information source.

SHS recommends that parents/guardians be responsible for the supervision of their student computer and internet activity while the student is not on the SHS campus and/or connected to the SHS Network.

D. Disclaimer

In accordance with the Children’s Internet Protection Act (“CIPA”), SHS uses filtering software to screen network traffic for offensive material. The Internet, as defined earlier, is a global network made up of many smaller contributing networks whose services are intended to support the open exchange of information. Students are cautioned that many internet websites contain

offensive, sexually explicit, and inappropriate material. Because no screening service is infallible, Servite is not responsible for search requests that may lead to sites with potentially inappropriate content. Additionally, having an e-mail address on the Internet may lead to receipt of unsolicited e-mail containing offensive or inappropriate content. Students accessing the internet do so at their own risk.

103 TERMS AND CONDITIONS

A. Acceptable Use of the SHS Network

SHS students may use the various resources provided by the SHS Network to pursue educationally-related activities. Students will be expected to follow generally accepted rules of network etiquette. Acceptable uses may include:

- Use appropriate language when communicating across the SHS Network and to the internet at large.
- Keep personal information, including the logins, passwords, addresses, and telephone numbers of other students and teachers confidential.
- Use available resources responsibly so as to not disrupt the quality of service to other students.
- Assume responsibility for the condition of his laptop computer:
 - Ensure the laptop remains clean and free of physical damage;
 - Do not intentionally or neglectfully place the laptop in a position to be damaged, destroyed, or stolen
 - Only install programs and visit websites that do not pose a virus or security risk to the laptop
 - Take care to update anti-virus definitions, update Microsoft Windows XP, run spyware/adware scans, etc.
 - Retain accountability for behavior on the SHS Network.
 - The student is in charge of his credentials (username, password) and how he uses available resources on the SHS Network
 - The student will be held accountable for reported violations of the Acceptable Use Policy.

B. Unacceptable Use of the SHS Network

Improper use of the SHS Network is prohibited. Actions that constitute unacceptable uses include, but are not limited to, the following:

- Violating any state or federal law, or local ordinance.
- Use of SHS network for, or in support of, prohibited activities including:
 - Use of the SHS Network for any obscene or pornographic purposes, including, but not limited to, the retrieving, viewing, or transferring of any sexually explicit material.
 - If a student inadvertently accesses such information, he should immediately disclose this access to a teacher or to a member of

the school administration. This will protect the user against allegations of intentionally violating this policy.

- Use of the SHS Network to store obscene or pornographic material or material acquired illegitimately including but not limited to: pirated games, movies, music, or other software.
- Making a statement of policy, either expressly or through implication, except for direct quotations, regarding SHS rules, procedures, documents published by SHS, or other official sources.
- Selling or purchasing illegal items or substances
- Causing or attempting to cause damage to others or their property, such as:
 - Use of the SHS Network for soliciting or distributing information with the intent to incite violence, cause personal harm or bodily injury, or to harass or 'stalk' another individual.
 - Deleting, copying, modifying, or forging other users' names, emails, files, or data; disguising one's identity; impersonating other users; sending anonymous e-mail
 - Damaging computer equipment, files, data, or the network in anyway.
 - Using profanity, obscenity, or generally offensive language in communication with persons of a particular race, gender, religion, sexual orientation, or to persons with disabilities.
 - Infringing on the protected rights of other individuals or organizations
- Plagiarizing any information gained on or through use of the SHS Network or any other network access provider
- Using copyrighted materials, including commercial software, without permission of the copyright holder, in violation of state, federal, or international copyright laws.
- Using the network or internet for commercial or non-SHS sanctioned activities.
- Using the SHS Network for financial gain or the transaction of commercial activities.
- Using Internet tools such as discussion boards, chat rooms, and instant messaging for other than educational purposes.
- Non-educational uses of the SHS Network including but not limited to: games, wagering, gambling, junk mail and private business activities.

C. Security Considerations

The SHS Network is password protected and students are given a unique password to access the network. Students are to always protect their passwords and immediately report any breaches of password security to their teacher, a member of the SHS Administration or to a Senior Staff Member of the Technology Department regardless if it is their own password or the password of another. Failure to report any incident promptly may subject the student to corrective action consistent with school disciplinary policies.

In order to maintain the security of the SHS Network, students are prohibited from engaging in actions including, but not limited to the following:

- Connecting to any other Internet Service Provider, (ISP) such as AOL, MSN, or SBC Yahoo, while connected to the SHS network.
- Connecting network components, such as routers, hubs, or access points to the SHS Network that are not explicitly owned and sanctioned by the SHS Technology Department.
- Intentionally disrupting the use of the SHS Network for other users, including, but not limited to:
 - Disruptive use of any processes or programs
 - Utilizing tools or methods such as keystroke logging or for ascertaining passwords
 - Engaging in “hacking” of any kind, which is defined as infiltrating a computer system without authorization.
 - Damaging or altering the software components of a computer or network system without authorization.
- Intentionally spreading computer viruses or spyware applications, such as Worms, Trojans, Phishing, etc.
- Disclosing the contents or existence of SHS network data files, confidential documents, e-mail correspondence, or other information to anyone other than authorized recipients.
- Sharing personal logins or passwords and unauthorized information regarding other users’ logins or passwords.
- Downloading unauthorized games, electronic media, and/or stand-alone applications from the internet that may cause a threat to the SHS Network.

D. Privileges and Rights Privacy

In accordance with the Family Educational Rights and Privacy Act (“FERPA”), SHS will protect all student data on its Network from unauthorized access by third parties, including but not limited to: transcripts, schedules, demographic and financial information, and data stored on the student’s network storage drive.

SHS will not guarantee the privacy of the student’s data from internal inspection by members of the SHS Administration. The student has no expectation of privacy regarding data tied to his identity, including but not limited to data stored on the student’s local hard disk drive and network storage drive.

The student also has no expectation of privacy regarding records of his activity while connected to the SHS Network, including but not limited to: documents produced, received and/or transferred, internet history, program history, and email communication.

- **Access**

All students will be granted equal access to the SHS Network until this agreement is violated. Students who either singly or repeated violate this Acceptable Use Policy are subject to a steady reduction in network privileges as well as other measures which are outlined in the Student Computer Disciplinary Code.

The use of the SHS Network is a privilege, not a right, and misuse of privileges associated with having a SHS Network account will be dealt with according to established SHS policy and the Student Computer Disciplinary Code.

- **Safety**

Servite strives to protect members of the SHS Community connecting to the SHS Network from harassment. Any community member who receives threatening or un-welcomed communication should immediately bring it to the attention of the SHS Administration or an IT department Senior Staff Member.

Students must, however, be aware that there are many services available on the internet that could potentially be offensive to certain groups or users. The Servite High School cannot identify and/or eliminate access to every offensive service. Students, then, must conduct themselves responsibly while connected to the SHS Network in order to preserve their safety.

104 ENFORCEMENT

A. Filtering

The SHS Technology Department has installed filtering software to control and report on user access to inappropriate and/or harmful material on the internet. The software can report on or restrict access to website addresses and content, e-mail, and programs that contain objectionable material. The definition of objectionable material is determined by the SHS Administration. Due to the dynamic and complex nature of internet, the SHS Network can not filter content completely, and the student is ultimately liable for responsible and appropriate internet browsing.

B. Monitoring

The SHS Network is routinely monitored to gauge the efficiency of all interconnected components. Students should again be reminded that any use of the SHS Network is subject to reasonable and appropriate monitoring by the Information Technology Department that abides by the requirements of all applicable state and federal laws. Any activities related to or in the support of violations of this policy and/or the Student Disciplinary Code may be reported and will subject the student to sanctions specified either in the Student Disciplinary Code or in this policy.

105 ASSUMPTION OF RISK

SHS will maintain the SHS Network and regularly update its available information to keep it reliable and accurate. However, the student and parent/guardian acknowledge that there is no warranty of any kind, either expressed or implied, regarding the accuracy, quality, or validity of any of the data available. The student uses the SHS network at their own risk. SHS does not warrant the SHS Network availability or reliability. SHS makes no guarantee that the SHS Network will be free of computer viruses.

The student further acknowledges that the information available through interconnecting networks may be inaccurate. SHS has no ability to maintain such information and has no authority over these materials. SHS makes no warranty of any kind, either expressed or implied, regarding the accuracy, quality, or validity of the data and/or information passing through the SHS Network from outside networks. Use of the SHS Network is at the risk of the student.

106 INDEMNIFICATION

The Parent/Guardian and student indemnify and hold SHS harmless from any claims resulting from the user's activities while utilizing the SHS Network that cause direct or indirect damage to the user, SHS, or third parties. In using SHS Network Resources, the Parent/Guardian student agrees to release SHS from all claims of any kind, including claims for direct or indirect, incidental, or consequential damages of any nature, arising from any use or inability to use the network, and from any claim for negligence in connection with the operation of the SHS Network.

107 SANCTIONS

Failure to abide by this policy may subject the student to corrective action ranging from suspension of some access privileges up to and including expulsion and prosecution according to the Student Computer Disciplinary Code.

The violator understands that if his privileges to use the SHS Network are restricted or revoked, he has the right to appeal the decision within ten (10) days, in writing, to the SHS Administration. The Administration's decision shall be FINAL. The violator understands that if his use of the SHS Network is restricted or revoked, there shall be no obligation to provide subsequent opportunity to access the SHS Network as extensively as before.

200 STUDENT COMPUTER DISCIPLINARY CODE (SCDC)

Introduction

At Servite High School, education thrives when parents, students, and teachers work together to achieve a powerful technology-based classroom learning environment. Computers are powerful tools, but can also present difficult distractions for students. The privilege of classroom tablet computer use is granted with high expectations of student discipline. Discipline will play a key role in determining the success of every student's educational technology experience.

The SHS Administration and Technology staff have worked together to produce a clear Acceptable Use Policy (AUP) including a Student Computer Disciplinary Code (SCDC), so that every student knows exactly what to expect. Parents and teachers are encouraged to discuss these guidelines with their students and are welcome to seek clarification from the SHS administration. Fully understanding and abiding by these codes will give each student the best opportunity to maximize his SHS learning experience.

In order to access Servite technology resources, all students and parents must accept in writing the provisions set forth in the Acceptable Use Policy (AUP) and the Student Computer Disciplinary Code.

Purpose

The purpose of the SCDC is to provide more specific information about common student behaviors that are considered inappropriate by the SHS administration. This list of prohibited behaviors and consequences is not intended to be exhaustive. There are behaviors not listed below that will result in sanctions according to the SHS AUP, but those listed below constitute the most common "pitfalls" or temptations that a student will face in the course of a school day at SHS.

The Technology Staff generates regular reports regarding prohibited student activities during the school day. Should a student's name show up on these reports, appropriate disciplinary measures will be taken. Students will be allowed no excuses and no exceptions for being found to have conducted themselves inappropriately. Students must refrain from performing prohibited actions during the school day, regardless of what class or free period they are in. Reports do not differentiate between class, lunch, activity period, and study hall. It simply provides a list of offenders who have taken particular actions during the period of time between the start of homeroom and the end of last period.

During this time, students are bound by all rules set forth in the Acceptable Use Policy and in this Disciplinary Code as outlined below. Students violating the AUP and SCDC will face a range of sanctions. These sanctions include detentions, monetary fines, and restrictions of access to technologies. Restricted access to the laptop and network resources will result in the student only being able to run programs and visit websites specifically essential to education at SHS that have been pre-approved by the administration. All listed penalties are minimum penalties for one-time offenses. Repeat offenders may see increased penalties at the discretion of the Dean of Students.

201 ACCESSING INAPPROPRIATE MATERIAL

The SHS Administration has the final authority over the decision of the quality or appropriateness of materials accessed by a student. Inappropriate material includes (but is not limited to) pornography, copyrighted media (games, pictures, movies, music, etc. to which a student does not own rights), non-educational images, and material related to avoiding or undermining SHS's network security and restrictions. Because this category contains a broad array of issues that range in severity, the consequences for violating this rule will also range in severity. Students should strive to use SHS technology resources for educational purposes only to avoid inappropriate behaviors.

202 IMPROPER NETWORK ACCESS

Student laptops are automatically configured to access the appropriate network resources that each student is authorized use of. During school hours, this will involve the student's School account connecting to the wireless or LAN network. Students are not permitted to establish ad hoc or peer to peer networks during school hours for any reason. Students are not permitted to connect their Home accounts to the SHS network AT ANY TIME – before during or after school. Students are not permitted to use proxy servers or any other tools to circumvent SHS Network security and content filtering. Students found to have accessed the network or internet improperly will face disciplinary action.

203 GAME-PLAY AND MESSAGING

During school hours, students are expected to use their computers exclusively for educational purposes. Students are prohibited from playing any games between the beginning of homeroom and the end of the day, whether in class or not. Locally installed, web based, flash, and network games are specifically prohibited. Students must keep all games and related materials on their home accounts. Games may not be installed on the school account for any reason. Students are prohibited from installing any chatting software (AOL Instant Messenger, Windows Messenger, ICQ, IRC, Trillian, etc.) on the "School" Operating System of their computers.

During school hours, students are prohibited from using web based chat programs as well as forums and bulletin boards not sanctioned by SHS. All communications are to take place via email or open discussion or as authorized by teachers for class use. Students are granted administrative abilities over their Home accounts as a privilege. Students are not to use these administrative rights to make changes to their School accounts (changing backgrounds, installing unauthorized programs, etc.). Students who abuse their Home administrative rights will have them suspended. Students found in violation of these rules will face disciplinary action.

204 COMPROMISING THE INTEGRITY OF CREDENTIALS

Electronic credentials (user name and password) are relied upon as trustworthy identification of individuals accessing technology resources. Password security is vitally important to the security of SHS technologies, and all students are responsible for the integrity, secrecy and safe-keeping of their own credentials. Students must use only the credentials individually assigned to them.

Any attempt to learn or compromise any password for any account that the student is not explicitly authorized to use will be treated as a very serious offense, as it compromises the security of SHS's network and its students. Students attempting to gain unauthorized access to SHS technologies will receive indefinite computer restrictions, will be presented to the Servite Administration for disciplinary review, and will be recommended for suspension or expulsion.

205 IRRESPONSIBLE USE OF TECHNOLOGY HARDWARE

SHS personnel have access to a vast array of very expensive and delicate technologies from network switches to laptops. All students are required to responsibly care for any hardware to which they have been entrusted access. Students will be held accountable for any damage to SHS technology items resulting from negligent, abusive, or irresponsible behavior.

The laptop is an expensive and delicate instrument whose care and safekeeping are explicitly the responsibility of the student. Each SHS student is entrusted with the care of his laptop. Students are required to keep their laptops on their person or secured in their lockers at all times. To prevent theft or damage, laptops should never be left unattended or unaccounted for. Careless treatment of SHS technology equipment may result in a disciplinary action. Damage caused to a student's personal laptop will be covered under the Accidental Damage Insurance Policy, but the student will have to pay the deductible cost particular to the damage before repairs are made. A list of deductible costs and procedures for obtaining insurance claimed repairs is attached to this form.

206 VIOLATING ACADEMIC INTEGRITY

Students will be held to a high standard of academic integrity. Students must only claim credit for work that they have completed themselves. Use of technology to misrepresent performance of school work will be considered a serious offense. Students caught using technology to cheat will be presented to the SHS administration for academic and disciplinary review.

Consent and Release Form

Servite High School
1952 W. La Palma
Anaheim, Ca. 92801

Please review the terms and conditions of the Acceptable Use Policy carefully. In accepting this policy, the student assumes responsibility for all privileges and duties associated with a SHS Network Account.

By signing below you are acknowledging that the student and parent/guardian have read and accepted the terms of this policy, Signatures are required from both student and parent/guardian for an account to be issued.

Student Consent:

I have read, reviewed and discussed the SHS Acceptable Use Policy. I agree with the terms and conditions outlined in this policy, understand the rights and responsibilities associated with having a SHS Network account, and will adhere to the provisions outlined in both this agreement and the Student Computer Disciplinary Code (“SCDC”).

Student Signature: X _____ **Date:** _____

Parent/Guardian Consent and Release:

I have read, reviewed and discussed the SHS Acceptable Use Policy with my son(s). I agree with the terms and conditions outlined in this policy and understand the rights and responsibilities my son(s) incur when given a SHS Network Account. I accept the provisions outlined in both this Acceptable Use Policy and the Student Computer Disciplinary Code.

I give the SHS Technology Department permission to issue my son(s) a SHS Network Account.

Parent/Guardian Signature: X _____ **Date:** _____