San Marcos Academy Acceptable Use Policy for Information Systems and Communication Resources

The following policy shall apply to all students, faculty, and staff of San Marcos Academy unless otherwise specified.

The purpose of this document is to inform families, students, and employees (*further referred to as "you", "your", or "user"*) of the policies and usage expectations while using technology resources at San Marcos Academy (*further referred to as "us", "we", or "SMA"*). By signing the Access Agreement form, ***you*** are agreeing to be legally bound by, and follow, the policies and rules set forth by SMA in this document.

The SMA communication system and associated resources; including but not limited to, Internet connection services (WAN), wired and wireless Local Area Networks (LAN), cloud-based networks, any telephonic system, SMA owned or licensed software, and any other interactive Electronic Communication Device (ECD)- will be referred to as **SMANet**. Electronic communication is a vital component to educational environment at SMA. This document covers the appropriate use of all ECDs, for employees and students at SMA, or any other person utilizing SMANet resources, either locally or remotely.

The primary purpose of SMANet; is to facilitate the exchange of information, and to further communication, education, and research consistent with classroom instruction and the school's curriculum and mission. SMANet is not for private or commercial business, anti-Christian, political or special interest group uses. The data transmitted, and files stored on SMANet or SMA's Google Apps for Education Domain (GAfE), are the property of SMA, and will be owned by us in perpetuity.

SMA hereby exercises and reserves the right to monitor, supervise, and limit the use of ECDs. SMA Administration will ensure that you have access to this policy, and have read and signed the Access Agreement, before you, the user, are issued a network account and allowed to use SMANet resources.

SMA Administration and the Director for Information Technology shall be responsible for maintaining and updating administrative regulations, procedures, and policies pertaining to the use of SMANet.

SAN MARCOS ACADEMY ACCEPTABLE USE POLICY

1.0 Overview

We are committed to protecting students, employees, partners and SMA from illegal or damaging actions by any group or individual, either knowingly or unknowingly. All SMANet resources are the property of SMA. SMANet resources, such as our student network 'ResNet', GAfE, and the Online Academy, are to be used for educational purposes; serving the interests of the school, faculty, and students; in accordance with the Student and Staff/Faculty Handbook and other policies set by SMA.

Effective security is a team effort, involving the participation and support of all SMA stakeholders: administrators, teachers, support staff, parents, and students, who deal with information and/or information systems. It is the responsibility of every user to know these guidelines and policies, and to conduct your activities accordingly.

SMA makes no guarantee that the functions or the services provided by or through SMANet will be error free or without defect. SMA will not be responsible for any damage users may suffer, including but not limited to; loss of data, interruptions of service, or criminal actions committed by you while using SMANet resources. SMA takes very seriously and will cooperate fully with all local, state, federal, and international law enforcement agencies in the matter of ANY cyber-crime. SMA is not responsible for the accuracy or quality of the information obtained through or stored on SMANet. SMA will not be responsible for financial obligations arising from unauthorized use of SMANet. Users can be assessed fees by SMA for infractions of this policy that result in interruption or perturbation of SMANet services.

Users understand and acknowledge that their use of SMANet resources can be visually and electronically monitored, logged, and/or reviewed at any time. Such data could be used as evidence to detect violations of this Acceptable Use Policy. Consequences for violations are outlined in section 6.0, "Enforcement" in this policy.

All users of SMANet will review this policy and a sign a new Acceptable Agreement page each year, upon hire or enrollment, or upon any major change in this document. After termination, graduation, or retirement, any user that retains access to SMANet resources is still bound by the previously signed agreement. SMA retains the rights to any data or communication a user creates even after that user no longer needs the use of SMANet resources for as long as we require.

2.0 Purpose

The purpose of this policy is to outline the acceptable use of the SMANet resources at San Marcos Academy. These rules are in place to protect the SMA community and San Marcos Academy. Inappropriate use exposes both you and San Marcos Academy to risks including virus attacks, compromise of network systems and services, and social or legal issues.

3.0 Scope

As defined in the introduction, the scope of this document covers the communication system and associated resources; including but not limited to, Internet connection services (WAN), wired and wireless Local Area Networks (LAN), cloud-based networks, any telephonic system, SMA owned or licensed software, and any other interactive Electronic Communication Device (ECD), will be referred to as **SMANet.**

This policy applies to all students, employees, contractors, consultants, temporaries, guests, and other individuals who utilize SMANet resources.

4.0 Guidelines

4.1 General Use and Ownership

1. While San Marcos Academy's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create or receive on SMANet remains the property of SMA. To protect SMANet, the administration cannot guarantee the confidentiality of information stored on any network or cloud-based device/service belonging to SMA, so that the user should have no expectation of personal privacy.
2. SMANet users are responsible for following the applicable SMA Handbook and exercising good judgment regarding the reasonableness of personal use. You must not engage in activities that will interfere with services provided to all SMANet users. This includes, but is not limited to, use of proxy or VPN software, disabling classroom monitoring software, sending or requesting any

communication of a sexual or any other inappropriate nature, propagating malware or spreading viruses, abusing or misusing the email or chat system "spamming", or any other illegal activity.

3. For security and network maintenance purposes, individuals authorized by San Marcos Academy may monitor equipment, systems, and network traffic at any time.
4. San Marcos Academy reserves the right to audit networks and computer systems on a periodic basis to ensure compliance with this policy, including any ECD owned or not owned by you.

4.2 Security and Proprietary Information

1. Users must take reasonable steps to prevent any unauthorized access to accounts or information.
2. Users will keep passwords secure and not share accounts. Authorized users are responsible for the security of their passwords and accounts. It is unacceptable to allow your password to be used by another user either intentionally or inadvertently, or to use another user's password. If you suspect your password has been compromised, you must immediately change your password or request password change assistance through SMA's IT department. Unauthorized usage of your account on ResNet is not only dangerous, it will increase your monthly internet usage, possibly causing you to incur usage fees as a result. See Section 8.0 "Charges for Service" for fees.

4.3 Unacceptable Use

1. Under no circumstances is any individual using SMANet resources authorized to engage in any activity that is illegal under local, state, federal, or international law.
2. Additionally the items listed in sections 4.4 and 4.5 are prohibited. Administrative and other authorized users may be exempt from these restrictions during the course of their legitimate job responsibilities. The restrictions listed below are by no means an exhaustive list.
3. Some of these rules may be suspended on a case-by-case basis via proper administrative authorization. Such authorization must be obtained in writing from the appropriate user's supervisor and administrator, and be approved by the Director of IT and/or the Network Administrator. Such access can be revoked without notice and at any time to protect SMANet resources.
4. At no time shall any user engage in any cyberbullying or any hate-related activities while employed at SMA or using SMANet resources.

4.4 System and Network Activities

The following activities are strictly prohibited:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent, or other intellectual property laws or regulations, or similar laws or regulations regarding intellectual property rights.
2. Unauthorized copying of copyrighted material.
3. Introduction of malicious programs to or from SMANet (e.g., viruses, worms, malware, etc.).
4. Revealing your account password to others or allowing use of your account by others.
5. Using SMANet to actively engage in procuring or transmitting material that is in violation of sexual harassment, child sex laws, or hostile workplace laws in the user's local jurisdiction.
6. Using SMANet to access, review, upload, download, store, print, post or distribute pornographic, obscene or sexually explicit material.
7. Causing security breaches or disruptions of network communication.
8. Executing or attempting to execute any form of network monitoring which will intercept data not intended for the user's computer.
9. Attempting to impersonate or represent another individual by sending forged information.
10. Users may not re-configure computer systems to impair or otherwise compromise their intended function or to make them partially or totally unusable by others.
11. Users may not modify any school owned ECD settings or wiring. This includes changing or installing any software. The user may not change their assigned computer name.
12. Users will not review or access any materials related to obtaining or using any controlled substance or products, which may not lawfully be used or consumed by minors.
13. Users will not circumvent user authentication or security of any SMANet resource or account.
14. Interfering with or denying service to any user.
15. Utilizing any proxy avoidance system; including VPN and darkweb software.
16. Attaching any type of file server to SMANet. This includes but is not limited to FTP, IRC, WWW, NOVELL, WINDOWS, DHCP or any gaming server. Any unauthorized device found on SMANet will be promptly disconnected and potentially confiscated.
17. Utilizing any peer-to-peer network services, such as Bittrorrent, uTorrent, etc.
18. Users are not allowed to set up or configure their own Wireless Access Point or router.
19. Users may not assign a specific "static" IP address or change the IP address of any workstation.
20. Students may not use a SMA owned computer designated for faculty or staff at any time.

4.5 E-mail and Communications Activities

The following activities are prohibited:

1. Sending unauthorized, unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam, mass email).
2. Any form of harassment via ECD or posting of inappropriate information to the Internet.
3. Students accessing social networking sites or chat rooms during school hours.
4. Posting to the web or through email inappropriate information (personal contact information, or school name or address).
5. Posting derogatory comments about other people or about SMA.
6. Inappropriate artwork, photographs, or unauthorized video or audio recording of SMA, SMA personnel or other students. This includes recording classroom activities without notifying the teacher prior to any recording taking place, or any unauthorized listening devices used by any staff member including smart phones or stationary listening devices or "bugs" without prior written consent of the student or employee.

5.0 Property Rights

San Marcos Academy has and hereby reserves the right to specify who uses its equipment and the information contained therein, under what circumstances, and to what purpose. SMA reserves the right to move or reassign equipment as needed. The use of SMA equipment (such as copy machines) and software (such as MS Office) for private or personal business is prohibited.

6.0 Enforcement

Any user found to have violated these guidelines, applicable laws and regulations, or posted classroom rules or Handbook rules; is subject to disciplinary action, up to and including, loss of SMANet privileges, fees, Disciplinary Review Board or dismissal (students), performance plans, or termination (employee), up to civil and/or criminal prosecution.

7.0 Definitions

Computer Virus - in computers, a virus is a program or programming code that replicates by being copied or initiating its copying to another program, computer boot sector or document. Viruses can be transmitted as attachments to an e-mail note or in a downloaded file, or be present on USB keys or CDs.

Cyberbullying - is the use of e-mail, instant messaging, chat rooms/applications, smart phones, or other forms of information technology; to deliberately harass, threaten, or intimidate someone.

Electronic communications device: Electronic communication device (ECD) means any type of instrument, device, machine, equipment or software that is capable of transmitting, acquiring, encrypting, decrypting or receiving any signs, signals, writings, images and sounds or intelligence of any nature by wire, radio, optical or other electromagnetic systems.

FTP: File transfer protocol, a standard Internet protocol, is a method to exchange files between computers on the Internet.

Gaming: Gaming is the running of specialized applications known as electronic games, especially on machines designed for such programs or using personal computers for online gaming.

IP Address - the most widely used level of the Internet Protocol (IP) today, an IP address is a 32-bit number that identifies each sender or receiver of information that is sent in packets across the Internet.

Local Area Network - A local area network (LAN) is a group of computers and associated devices that share a common communications line or wireless link.

Peer to Peer - On the Internet, peer-to-peer (referred to as P2P) is a type of transient Internet network that allows a group of computer users with the same networking program to connect with each other and directly access files from one another's hard drives.

Pirated Software - Software piracy is the illegal copying, distribution, or use of software.

ResNet-The wired or wireless network students use to connect to the internet.

Router - a router is a device or, in some cases, software in a computer, that determines the next network point to which a packet should be forwarded toward its destination.

Social Networking: social networking is the practice of expanding one's business and/or social contacts by making connections through individuals or groups- specifically using the Internet **Spam:** Unauthorized and/or unsolicited electronic mass mailings.

Wireless Access Point - a station that transmits and receives data (sometimes referred to as a transceiver). An access point connects users to other users within the network and also can serve as the point of interconnection between the wireless and a fixed wire network. The number of access points a wireless network needs is determined by the number of users and the size of the network.

8.0 Charges for Service

1. Operating System Reinstallation Fee- A technology fee can be assess for student accounts if a student intentionally disables their operating system, particularly for repeat offenders.
2. Out of Warranty Repair Fee- A technology fee that can be assessed for complicated repairs facilitated on out of warranty systems through the manufacturer, if agreed to by the parent or guardian by signing the Out of Warranty repair agreement
3. Damage to SMANet Fee- This is a discretional fee if any user is found to have damaged the functionality of SMANet, you can be charged at the rate of the IT professional (including SMA IT staff or contractors) required to resolve or repair the damage.
4. Overage Fee- Overage Fee- In order to meet the needs of Academy students, faculty and staff; Wi-Fi internet is available in most areas of campus. There is no charge for internet service up to the base usage, please see the table of fees for the current base usage and per Gigabyte overage.

9.0 Revision History

Revised 07/28/09 by Executive Council for approval of Board of Trustees

Revised 08/13/09 to add definitions

Revised 08/18/09 to modify 4.4 System and Network Activities

Revised 08/26/10 to modify 4.4 System and Network Activities and for paragraph formatting

Revised 06/27/12 to modify business name and designate fewer restrictions on ResNet

Revised 07/18/13 to modify allowable activities and clarify some definitions

Revised 08/01/14 to adjust usage cost structure and clarify some definitions

Revised 06/18/16 Major revision change to version 2.0 routing for approval