ST. JOSEPH ACADEMY
(SJA)

Department:	Information Technology
Number:	210.2
Effective Date:	October 19, 2015
Review Date:	March 26, 2021
Revised Date:	March 3, 2020
Page:	1 of 3

I. Policy:

The purpose of this policy is to outline acceptable and unacceptable use of electronic devices and network resources at St. Joseph Academy (SJA), in conjunction with its established culture and ethical behavior, openness, trust and integrity.

SJA provides computer devices, smartphones, networks, and other electronic information systems to meet mission, goals, and strategic initiatives. SJA must manage these assets responsibly to maintain the confidentiality, integrity, and availability of its information assets. This policy requires the users of information assets to comply with company policies and protects the company against damaging legal issues.

II. Procedures:

A. All employees, contractors, consultants, temporary and other workers at SJA, including all personnel affiliated with third parties must adhere to this policy. This policy applies to information assets owned or leased by SJA, or to any device that connects to the SJA computer network.

B. You are responsible for exercising good judgment regarding appropriate use of SJA resources in accordance with SJA policies, standards and guidelines. SJA resources may not be used for any unlawful or prohibited purpose.

C. For security, compliance, and maintenance purposes, authorized personnel may monitor equipment, systems, e-mail, Internet use, and network traffic at any time. Personal devices that interfere with other devices or users on the SJA network may be disconnected without advanced notice.

<u>System Accounts:</u>

D. You are responsible for the security of data, accounts, and systems under your control. Keep passwords secure and do not share account or password information with anyone, including other personnel, students, family, or friends. Providing access to another individual, either deliberately or through failure to secure its access, is a violation of this policy.

E. You must maintain passwords in accordance with the requirements set forth by SJA. The passwords will be of at least medium complexity and will be changed at least annually.

F. You must ensure through legal or technical means that proprietary information remains within the control of SJA at all times. Conducting SJA business that results in the storage of proprietary information on personal or non-SJA controlled environments, including devices maintained by a

third party with whom SJA does not have a contractual agreement, is prohibited. This specifically prohibits the use of an e-mail account that is not provided by SJA for company business.

Computing Assets

G. You are responsible for ensuring the protection of assigned SJA assets.

H. All laptops, smartphones, tablets, and workstations must be secured with a password, PIN, or biometric system for access. All devices should require re-authentication when not in use for a period of 10 minutes or less. All devices must be locked or logged off when the device is unattended.

I. Non SJA owned devices such as bring your own device (BYOD) that connect to the SJA network must be approved by the SJA Systems Administrator and your immediate supervisor prior to use.

J. Do not interfere with corporate device management or security system software, including, but not limited to, system updates and Malware protection.

Computer Usage

K. It shall be considered a breach of this policy to use your computer(s) and the Internet to stream music from any site. Pandora or similar sites may be used to play music in classrooms only during nap time.

L. Downloading ANY software other than safe educational or productivity software/materials is prohibited.

M. Customizing the Standard issued computer setup with downloaded games, software, etc. may cause the computer to become unstable. The individual user is responsible for maintaining an appropriate and safe operating environment on their computer(s). Repeated attempts by the IT Department to "Fix" computer problems related to this type of activity shall be considered a breach of this Policy.

N. It is the responsibility of each Teacher or Caregiver to monitor the activity of any Student or child using SJA computer equipment, giving special attention to the older children that may represent a greater threat for misuse of the equipment.

O. All classroom computers will be reformatted annually to provide a clean starting point at the beginning of each school year. Teachers should not store files permanently on computers and not have the expectation that the files will be there the following year.

P. It shall be considered a breach of this policy if you employ or use outside help such as a spouse, friend, family member, etc. to help with IT-related issues to include moving and reassembling of computer equipment. Do not attempt to troubleshoot complex IT issues yourself. Instead, utilize IT Department resources to resolve these issues.

Network Use and Electronic Communications

Q. You are responsible for the security and appropriate use of SJA computer network assets under your control. Using SJA resources for the following is strictly prohibited:

a) Causing a security breach to either SJA or other network resources, including, but not limited to, accessing data, servers, or accounts to which you are not authorized.

b) Violating copyright law, including, but not limited to, illegally duplicating or transmitting copyrighted pictures, music, video and software.
c) Use of the Internet or SJA network that violates the SJA Internet and E-Mail Usage Policy, SJA Policies, or local law.
d) Using unsecured Wi Fi to conduct SJA business
e) Employees shall not consider it their right to utilize SJA's wireless network for personal device use (BYOD) such as connecting a cell phone to avoid data use charges.
f) SJA provides a robust wireless network infrastructure intended to enhance the School's computing environment and provide a more clutter-free facility. Using the wireless network in any way that may compromise or harm the organization is strictly prohibited.

Electronic Communications

The following are strictly prohibited:

R. Inappropriate use of communication vehicles and equipment, including, but not limited to, supporting illegal activities, procuring or transmitting material that violates SJA policies against harassment or the safeguarding of confidential or proprietary information.

S. Sending spam via e-mail. Sending inappropriate text messages, pages, instant messages, voice mail, or other forms of electronic communication.

T. Forging, misrepresenting, obscuring, suppressing, or replacing a user identity on any electronic communication to mislead the recipient about the sender.

U. Use of SJA e-mail or IP address to engage in conduct that violates SJA policies or guidelines. Posting to a public newsgroups, bulletin boards, or any social media with an SJA e-mail or IP address represents SJA to the public; therefore, you must exercise good judgment to avoid misrepresenting or exceeding your authority in representing the opinion of the company.

V. Using Social Media to convey personal agendas not consistent with SJA's core values (please refer to our *Social Media Use Policy*).

Enforcement

W. A user found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment by SJA.

Approved by: _____ Date 3/29/24
President/CEO