St. Joseph School
Electronic Information Access and Use For Educational Purposes Policy

St. Joseph (the "School") encourages and strongly promotes the use of electronic information technologies in educational endeavors. The School provides access to electronic information resources in a variety of formats, and for the development of information management skills. Together these allow learners to access current and relevant resources, provide the opportunity to communicate in a technologically rich environment and assist them in becoming responsible, self-directed, lifelong learners.

The School has developed this Electronic Information Access and Use For Educational Purposes Policy (this "Policy") to govern the access, use and security of School Systems (defined below). Every User (defined below) must read, sign, and abide by this Policy.

For the purposes of this Policy, the following capitalized terms have the meanings ascribed to them below. Additional capitalized terms are defined within this Policy.

(a) "PEDs" means portable electronic devices, including, without limitation, laptop computers, chrome books, cellular telephones, pocket personal computers, handheld computers, cameras, video recorders, sound recording devices and all forms of personal digital assistants ("PDAs").
(b) "School Confidential Information" means all confidential and/or proprietary information and materials of the School, its faculty, administrators, students, employees and/or third parties with which the School does business.
(c) "School Electronic Information" means all electronic information (including the School Confidential Information), communications or activity created, sent, received, stored and/or otherwise used on behalf of the School, whether or not the School Systems are used to create, send, receive, store or otherwise use that information or those communications. The School Electronic Information includes voicemail messages on the School Equipment.
(d) "School Equipment" means any and all electronic devices owned, leased or operated by or for the benefit of the School, which have the capability of creating, sending, receiving, storing and/or otherwise using electronic information, materials and/or communications, including, but not limited to, pagers, computers, chrome books, servers, disk drives, scanners, photocopiers, printers, fax machines, telephones and PEDs. School Equipment includes all operating software, application software and firmware owned and/or licensed by the School, which resides and/or is embedded in any School Equipment.
(e) "School Networks" means all School voice and data systems, including, without limitation, the School's Internet, intranet and extranet systems.
(f) "School Systems" means the School Equipment and the School Networks.
(g) "Users" means any individual who accesses and/or uses School Systems, including, without limitation: (i) School full time, part-time and temporary faculty and/or employees; (ii) School third party contractors, vendors, consultants, representatives and agents, as well as their full time, part-time, and temporary employees; and (iii) parents, students, and volunteers.
(h) "User Equipment" means electronic devices that are continuously or intermittently connected to School Systems, or a component thereof, which are not owned or leased by the School, including, without limitation, User-owned computers, pagers, chrome books, telephones, fax machines, and PEDs. User Equipment without connectivity to School Systems does not fall under the purview of this Policy.

This Policy applies to all Users and to all School Systems, User Equipment, School Confidential Information and School Electronic Information.

To the extent this Policy applies to School faculty and/or employees, this Policy supplements, but does not replace, the School's (policies/handbook/manual). The terms of this Policy will govern any conflict or inconsistencies with the terms of such (policies/handbook/manual). Any School faculty and/or employee who violate this Policy may be subject to disciplinary action, up to and including termination.

To the extent this Policy applies to students, this Policy supplements, but does not replace, the School's Code of Conduct. The terms of this Policy will govern any conflict or inconsistencies with the terms of such Code of Conduct. Any student who violates this Policy may be subject to disciplinary action, up to and including suspension and/or expulsion.

To the extent his Policy applies to third parties, this Policy supplements, but does not replace, School's agreements with such third parties. The terms of this Policy will govern any conflict or inconsistencies with the terms of such agreements. Third parties who violate this Policy may no longer be considered eligible for access to and/or use of School Systems, School Confidential Information and/or School Electronic Information. A third party's violation of this Policy shall also be considered a material breach of its agreement with School, entitling School to terminate such agreement for cause.

The School Systems, School Confidential Information and School Electronic Information are the School's property and may be used solely for educational purposes and/or the School's operational activities. Each User must take all necessary steps to prevent unauthorized access to or use of School Confidential Information and School Electronic Information. Unless otherwise directed by School, or permitted or required by this Policy, Users may not: (a) take, retain or use School Confidential Information and/or School Electronic Information for User's own benefit; (b) disclose School Confidential Information and/or School Electronic Information to any other entity or unauthorized person without the written permission from a School officer; (c) delete, encrypt, password protect, or retain electronic files containing School Confidential Information and/or School Electronic Information (including emails and attachments); or (d) take any other action that impairs, restricts, limits, or impedes School's ability to have full access to and use of its School Confidential Information and/or School Electronic Information. Upon request, User shall return to School all School Confidential Information and/or School Electronic Information, and otherwise fully cooperate with and assist School in ensuring School's ability to have full access to and use of School Confidential Information and/or School Electronic Information. Such cooperation and assistance may include, but is not limited to, removing any password protection, encryption or other proprietary format on School Confidential Information and/or School Electronic Information.

The School retains the right to search, monitor, access, and/or review all School Systems, School Electronic Information and all other electronic and voice mail communications, computer files, databases and any other electronic transmissions contained in or accessed by School Systems, at any time, with or without notice, at School's sole discretion. This may include, without limitation: (a) viewing, printing, downloading, and/or listening to emails and voicemails created, sent, received, stored, and/or otherwise used in or through School Systems; (b) viewing, modifying and/or removing a User's electronic mailbox; and/or reviewing audit trails created by School Systems.

No email, voicemail or other information, whether received, sent, stored or used on or through School Systems, is private. Users have no expectation that any information contained on any School Systems is confidential or private to them. The School's System is not a public forum and access to the technology is a privilege and not a right. By using School Systems, Users consent to the access and disclosure of email messages, voicemail messages and other information within School's organization without restrictions, but subject to School's legal and contractual obligations of confidentiality. Users should not use School Systems to create, send, receive, and/or store information that is personal if it is confidential or sensitive, since such personal information will be considered School Electronic Information if created, sent, received, and/or stored using School Systems.

The School makes no warranties of any kind, whether expressed or implied, for any reason regarding the access to, or use, quality or availability of, School Systems, including but not limited to the loss of data. All School Systems are provided on an "as is, as available" basis.

School Responsibility

The School will designate a system administrator who will manage the School Systems and make the final determination as to what is inappropriate use based on this Policy. The system administrator may close an account at any time for infractions or temporarily remove a User account and/or a User's access to or use of the School Systems for anu reason, including, without limitation, to prevent unauthorized activity.

The School will implement filtering software intended to block minors' access to materials that are obscene, child pornography, harmful to minors, or that the School determines to be inappropriate for minors. However, the School does not guarantee that it will be able to fully prevent any User's access to such materials, or that Users will not have access to such materials while using School Systems. The filtering software operates only within the School wide area network (WAN) or local area network (LAN). The filtering software does not operate during dial-ups access.

The School does not take responsibility for resources located or actions taken by any Users that do not support the purposes of the School.

It shall be the responsibility of all members of the School staff to supervise and monitor usage of the School Network and access to the Internet in accordance with this Policy and the Children's Internet Protection Act.

Saint Joseph Network Users

Users will be granted access to appropriate services offered by the School Network. In addition, the following people may become account holders or members of the School Network.

1. Students: Students who are currently enrolled in the School may be granted a School Network account upon agreement to the terms stated in this Policy.
2. Faculty/Staff: Staff members currently employed by the School may be granted a School Network account upon agreement to the terms stated in this Policy.
3. Others: Anyone may request a special account on or use of the School Network. These requests will be granted on a case-by-case basis, depending on need and resource availability.

Privileges and Responsibilities of Users

Privileges:

Subject to the terms of this Policy, Users have the privilege to:

- Use all authorized School Systems for which they have received training to facilitate learning and enhance educational information exchange.
- Access information from outside resources which facilitate learning and enhance educational information exchange.
- Access School Networks and the Internet to retrieve information to facilitate learning and enhance educational information exchange.

User Responsibilities

Users are responsible for:

- Using School Systems only for facilitating learning, appropriate personal growth and enhancing educational information exchange consistent with the purposes of the School.
- Attending appropriate training sessions in the use and care of School Systems.
- Seeking instruction for the use of any available technology with which they are not familiar.
- Adhering to the rules established for the use of School Systems, in the School or through remote access outside of the School.
- Refraining from disclosing, using or disseminating personal identification information regarding students over the Internet without parent or guardian authorization.
- Maintaining the privacy of passwords and are prohibited from publishing or discussing passwords. School Network accounts are to be used only by the authorized owner of the account for the authorized purposes.
- Students may use e-mail, chat, instant messaging, and other forms of two-way electronic communications only for educational purposes and only under the direct supervision of an adult.
- Having all electronic media scanned for virus, dirt, damage or other contamination which might endanger the integrity of School Systems before they are used in School Systems.
- Material received, created or distributed using School Systems.
- Maintaining the integrity of the electronic messaging system (voice, e-mail, etc.), deleting files or messages if they have exceeded their established limit, reporting any violations of privacy and making only those contacts which facilitate learning and enhance educational information exchange. If a User remains in non-compliance, the system administrator may delete files and messages, freeze the account, and/or close the account.
- Preventing material considered pornographic by the School, inappropriate files or files dangerous to the integrity of the School's Systems from entering the School via the Internet or from being reproduced in visual, digital or written format.

- Awareness of the adhering to copyright laws and guidelines and trademark laws and applicable licensing agreements in the use of School Systems and in the transmission or copy of text or files on the Internet or from other resources. Users must also comply with all other applicable laws, both state, and federal, with respect to their use of the School's Systems.
- Using caution (Buyer Beware) when considering the purchase of goods or services over the Internet. The School is not liable for any financial obligations made or any personal information provided while using School Systems.
- Financial restitution for unauthorized costs incurred or damages or repair necessitated by inappropriate use or access.
- Any damages to, or incurred on, User Equipment. Users accessing School Systems on User Equipment do so *at their own risk.*
- Abiding by the rules set forth in this Policy, general School rules, and additional rules as may be established by the School. Local School Committee policies, staff manuals, departmental procedures, and student handbooks may include such rules.

Users are prohibited from:

- Using the technology for a "for-profit" business, for product advertisement or political lobbying.
- The malicious use of technology to disrupt the use of technology by others, to harass or discriminate against others and to infiltrate unauthorized computer systems.
- Using School Systems to draft, send, or receive inappropriate communications and material including but not limited to, items which are pornographic, obscene, profane, vulgar, harassing, threatening, defamatory or otherwise prohibited by law.
- Participating in hate mail, harassment, discriminatory remarks and other antisocial behaviors on the network.
- Vandalism includes, but is not limited to, the creation or intentional receipt or transmission of computer viruses.