St Monica School, B'Kara

SCHOOL STAFF TECHNOLOGY POLICY

Maintaining the security and confidentiality of information and protecting St. Monica School B'Kara, hereafter referred to as the SCHOOL. The SCHOOL's concern in this regard is heightened by the various technology resources provided to its employees to facilitate the creation and communication of businessrelated information in the most effective and efficient manner possible. In light of these concerns, this Policy has been developed, which establishes the parameters for technology resources usage and serves to enhance employee awareness of our obligation to hold certain information confidential, and to protect the integrity of the SCHOOL's property and interests. This Policy supplements all existing federal, state, local, laws, regulations, agreements, and contracts, and any other SCHOOL policy, which currently apply to information confidentiality and technology resources. Users who do not comply with this Policy are subject to discipline, including, without limitation, revocation of technology usage and, up to and including, termination.

Scope of The Policy

This Policy applies to all St Monica School, B'Kara employees and other persons who are authorized to use the SCHOOL's technology resources, including certain consultants, contractors, vendors, students, and interns ("users"). This Policy applies to the following forms of technology resources and the information created by their use, including but not limited to (1) computers (including desktop, laptops, portable, servers, mainframes, local area networks, wide area networks, printers, software and removable storage media (e.g., floppy disks, CD-ROMs, hard disks and tape)); (2) electronic mail ("e-mail"), including attachments; (3) the Internet, (4) the phone systems, and (5) anything connected to or apart of the SCHOOL's server. The term "the SCHOOL's Technology Resources" is meant to include any of the aforementioned, specifically, and any other computer-related or technology-related device that is or may be owned, rented, or leased by the SCHOOL.

THE POLICY

1. The SCHOOL's Technology Resources May Be Used Only For Legitimate, Business-Related Reasons.

The SCHOOL's technology resources may be used only for legitimate business-related reasons.

The SCHOOL's technology resources may not be used to conductpersonal business of any kind, without expressed permission from a supervisor or administrator at the SCHOOL.

All information that is entered, created, received, stored or transmitted via the SCHOOL's technology resources, including all e-mail messages, are and will remain the SCHOOL's property. Such information may neither be used for any purpose unrelated to the SCHOOL's business nor sold, transmitted, conveyed or communicated in any way to anyone outside of the SCHOOL other than for business-related reasons.

2.   No Expectation of Privacy

Users should have no expectation of privacy in connection with the entry, creation, transmission, receipt, or storage of information via the SCHOOL's technology resources. Users waive any right to privacy in information entered, created, received, stored or transmitted via the SCHOOL's technology resources, and consent to access and disclosure of such information by authorized personnel.

As with all other property, the SCHOOL technology resources and all information entered, created, transmitted, received or stored via our technology resources is subject to inspection, search and disclosure without advance notice by persons designated or acting at the direction of the SCHOOL or as may be required by law or as necessary to ensure the efficient and proper administration and operation of our technology resources. For example, authorized persons may inspect, search and disclose such information to investigate theft, disclosure of confidential business or proprietary information, personal abuse of the system, or to simply monitor work flow or productivity. This monitoring and/or search includes, without limitations, the individual hard drives of any computer owned, leased, rented, or maintained by the SCHOOL, any information stored on any hard drives owned, leased, rented, or maintained by the SCHOOL, which may include emails to or from any SCHOOL issued email account, or any personal account that may be accessed from a the SCHOOL computer, any documents drafted on the SCHOOL's computer, any internet sites accessed, and/or any phone calls made or received from any phone systems owned, leased, rented, or maintained by the SCHOOL, and any messages left on any phone owned, leased, rented, or maintained by the SCHOOL.

Because the SCHOOL is sensitive to employee concerns, it will make every effort to ensure that all such inspections are conducted professionally and ethically. Users, however, must recognize that authorized persons have the ability to track and monitor all information sent internally and externally to the SCHOOL via technology resources at any time for any reason. Users should have no expectation of privacy in any of the work that is performed on any SCHOOL computer, with any emails transmitted or received (or accessed) on a SCHOOL computer, any internet site accessed on a SCHOOL computer, or with respect to any phone call received or made to/from any SCHOOL phone system, or any messages left on any SCHOOL phone system.

All passwords and security used in connection with the SCHOOL technology resources are the SCHOOL's property and must be available to the SCHOOL, upon request, for any reason. Users should understand that their use of passwords does not preclude authorized persons to access the SCHOOL's technology resources.

3. The Creation or Transmission of Any Information That May Be Construed To Violate the SCHOOL's Harassment-Free Workplace Policy or Equal Employment Opportunity Policy Is Strictly Prohibited

Users are strictly prohibited from using the SCHOOL's technology resources in any way that may be offensive to others. This prohibition includes, for example, the transmission of sexually explicit or obscene messages or cartoons, ethnic or racial slurs, or anything that may be constructed unlawful harassment or disparagement based on race, color, religion, sex, national origin, age, disability, ancestry, sexual orientation, marital status, parental status, source of income, military discharge, or any other status protected by law. Relatedly, users may not use technology resources to transmit critical or derogatory statements regarding individual employees, clients, consultants, contractors, vendors, students, volunteers or residents. Users violating these prohibitions may be subject to disciplinary action, up to and including termination.

4.   Use of the SCHOOL'S Technology Resources Is Subject To the SCHOOL's NoSolicitation/No-Distribution Policy

The SCHOOL's policy strictly forbids employees from soliciting, during their working time or the working time of the employee being solicited, any other employee to support any individual or organization. It also forbids employees from distributing any literature on behalf of any individual or organization on SCHOOL property. This includes the distribution of chain letters of all kinds.

5.   Intellectual Property (Copyright and Patent) Laws and Computer Standards

Users may not violate any copyright, patent or other intellectual property law, including restricted software laws. Accordingly, unless permission has been expressly and officially provided, users may not post or download any information protected by copyright or patent law. If copyright, patent or other ownership status is unknown, users may not post, upload, download or otherwise use any information, content, software or other property and should consult the network administrator with any inquiries.

6.   Viruses

All SCHOOL technology resources must be protected from accidental destruction or deliberate attempts at sabotage by computer viruses. Users thus may not introduce virus-infected files or media into the SCHOOL's technology resources. Users must make all reasonable efforts to ensure that all files accessed or collected are virus-free and should minimize downloading workrelated information unfamiliar from the Internet and via e-mail. Users should use discretion when receiving e-mail from unknown sources, especially where the e-mail contains attachments. Prior to placing any file on the SCHOOL's network, users must scan for viruses using up-todate, approved virus scanning software.

7.   Confidential Information

Users must take every measure to ensure that confidential SCHOOL information, and information otherwise protected is entered, created, received, stored or transmitted via technology resources remains confidential and private.   Likewise, users must continue to respect the confidentiality of any report containing confidential information while handling, storing, and disposing of these reports in an appropriate manner.

Users are prohibited from searching for using, sending, posting or otherwise disclosing confidential information or information protected by the attorney-client privilege to any individual for any non-work or business related reason, without partner permission.

8.   Encryption

To ensure continuous access to technology resources users shall not use personal hardware or software to encrypt information entered, created, received, stored or transmitted via technology resources.

9.   Internet Use

Like all other technology resources, the SCHOOL provides Internet access only for legitimate business-related, education, research, outreach, and administrative purposes. The Internet shall not be used for any personal use.

10.   Social Media

Social Media includes any website or medium (including video) that allows for the electronic and digital communications in cyberspace, which includes, but is not limited to, email, internet, text messaging, Facebook, Twitter, LinkedIn, YouTube, MySpace, Hudl, Formspring, and blogs. A

policy has been developed to protect you and the SCHOOL'S exposure and liability, while also providing you an opportunity to share educational forums and ideas with others.

The use or accessing of social media at work is not permitted without expressed written authorization from a supervisor or administrator at the SCHOOL.

When using social media within a written authorization through the SCHOOL, or using social media outside of working hours on your own time, any use **must be** consistent with our **mission**, **purpose**, and **values**. All employees must use social media within the guidelines set forth in the employee handbook and/or rules of conduct. Violations of the the policy, no matter how small, can and will be subject to discipline as outlined fully in the employee handbook.

You are personally responsibility for what you post. Remember that what you post can often be viewed by both personal and professional contacts. Post responsibly. If you publish content related to the SCHOOL on any non-SCHOOL operated or sponsored site, you must state that "the views on this post are my own and not necessarily those of St Monica School. Additionally, with all posts on any social media site you must abide by the following:

- Do not publish any confidential or proprietary information on a social site;

- Do not discuss the SCHOOL, the SCHOOL employees, vendors, clients, or other partners of the SCHOOL, without written authorization;

- Do you use insults, obscenity, racial slurs, ethnic slurs, or any other negative comments that can be construed in any way as discriminatory or harassing;

- Do not post photographs taken any SCHOOL-sponsored events; and

- Respect all copyright, fair use, and financial disclosure laws;

11.   Other Communications

Communications between school personnel and students outside of school shall be limited to traditional, organization-authorized methods such as organization-issued email accounts, and should only be conducted for organization-related purposes. Accordingly, the following communication and contact between retreat personnel and minor is prohibited:

- Calls to a minor's personal phone,
- Texting,
- Communication through messaging services such as Instant Messenger,
- Communication through personal social networking accounts, including "friending," and
- Communication through personal email accounts.

Should communication outside of traditional, organization-authorized methods be necessary, the administration should be notified of the communication and its purpose, and the communication should be documented by the personnel member.

12.   Violations

Violations of any of the above policies by personnel shall be subject to discipline, up to and including, termination.

I, _____, hereby certify and declare that I have read (insert SCHOOL NAME'S) <u>COMPUTER-USAGE AND SOCIAL MEDIA POLICY</u>. By executing this document, I am certifying that I understand the Policy, and all of the terms contained therein, and agree to abide by the terms and provisions contained within the Policy.

By: _____

Date: _____