ISLAMIC CENTER OF AMERICA
Madrasatu Ahlis Sunnah
215 North Oraton Parkway
East Orange, N.J. 07017
(973) 672-6690
www.thesunnah.org/school

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

Information and Technology Security Policy

Maintaining the authorized accessibility, security, and confidentiality of information and protecting Islamic Center of America/Madrasatu Ahlis Sunnah's (also referred to herein as "the organization") technology is a paramount concern of the organization. The organization's concern in this regard is heightened by the various technology resources provided to its employees/volunteers to facilitate the creation and collaboration around business-related information in the most effective and efficient manner possible. Considering these concerns, this policy has been developed to establish the parameters for technology resource usage and to enhance employee awareness of our obligation to hold certain information confidential and to protect the integrity of the organization's property and interests. This Policy supplements all existing federal, state, and local laws, regulations, agreements, contracts, and any other organization policies that 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, civil/criminal penalties as appropriate, and termination.

Scope of The Policy: This Policy applies to all the organization's employees and other persons who are authorized to use the organization's technology resources, including volunteers, consultants, contractors, vendors, students, and interns (also referred to herein as "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., USB Drives, CD-ROMs, hard disks, and tape)); (2) electronic mail ("e-mail"), including attachments; (3) the Internet; (4) phone systems; and (5) anything connected to or a part of the organization's server or cloud accounts (also referred to herein as "systems").

THE POLICY

The organization's Technology Resources May Be Used Only for Legitimate, Business-Related Reasons The organization's technology resources may not be used to conduct personal business of any kind without express written permission from a supervisor or administrator at the organization. Supervisors must consult the Technology Department to discuss the impact on systems by the potential use. The Technology Department must discuss the details of the request with the board.

All information that is entered, created, received, stored, or transmitted via the organization's technology resources, including all e-mail messages, is and will remain the organization's property. Such information

may neither be used for any purpose unrelated to the organization's business nor sold, transmitted, conveyed, or communicated in any way to anyone outside of the organization other than for business-related reasons.

No Expectation of Privacy

As all information created or residing on the organization's systems belongs to the organization, users should have no expectation of privacy in connection with the entry, creation, transmission, receipt, or storage of information via the organization's technology resources. Users waive any right to privacy in information entered, created, received, stored, or transmitted via the organization's technology resources and consent to access and disclosure of such information by authorized personnel for authorized reasons.

As with all other property, the organization's technology resources and all information entered, created, transmitted, received, or stored via our technology resources are subject to inspection, search, and disclosure without advance notice by persons designated or acting at the direction of the organization 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 personnel may inspect, search, and disclose such information to investigate theft, disclosure of confidential business or proprietary information, personal abuse of the system, or to monitor workflow or productivity.

This monitoring and/or search includes, without limitation, the individual hard drives of any computer owned, leased, rented, or maintained by the organization, any information stored on any hard drives owned, leased, rented, or maintained by the organization, which may include emails to or from any organization-issued email account, or any personal account that may be accessed from an organization computer, any documents drafted on the organization'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 organization, and any messages left on any phone owned, leased, rented, or maintained by the organization.

Because the organization 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 personnel can track and monitor all information sent internally and externally to the organization via technology resources at any time for any reason. Users should have no expectation of privacy in any of the work performed on any organization computer, with any emails transmitted or received (or accessed) on the organization computer, any internet site accessed on the organization computer, or with respect to any phone call received or made to/from any organization phone system, or any messages left on any organization phone system.

All passwords and security used in connection with the organization's technology resources are the organization's property and must be available to the organization, upon request, for any reason.

Users should understand that their use of passwords does not preclude authorized personnel from accessing the organization's technology resources for authorized reasons.

Technology Department personnel do not have the right to view any information unless it is necessary for conducting their jobs. Any request for investigations that may require entering shared department folders/drives or other resources must have written board approval.

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

Users are prohibited from using the organization'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 construed as 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.

Use of the Organization's Technology Resources Is Subject To the Organization's No-Solicitation/No-Distribution Policy

The organization's policy 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 the organization's property. This includes the distribution of chain letters of all kinds.

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.

Viruses

All the organization's 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 organization's technology resources.

Users must make all reasonable efforts to ensure that all files accessed or collected are virus-free and should minimize downloading work-related 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 organization's network, users must scan for viruses using up-to-date, approved virus scanning software.

Confidential Information

Users must take every measure to ensure that confidential organization 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 attorney-client privilege to any individual for any non-work- or business-related reason, without written permission. Legal action may be taken against violators of this policy.

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. If organization information is to be passed to authorized external organizations for an authorized business reason, it must be encrypted before transmission using approved encryption software. Engage the Technology Department for help.

Internet Use

Like all other technology resources, the organization provides Internet access only for legitimate business-related, education, research, outreach, and administrative purposes. The Internet shall not be used for any personal use. Incidental personal uses, for example, to check a personal email account while on a break, will not violate this policy. If you are not sure if your behavior will violate the policy, please ask your supervisor for direction.

Social Media

Social Media includes any website or medium (including video) that allows for electronic and digital communications in cyberspace, which includes, but is not limited to, email, internet, text messaging, Facebook, Twitter, LinkedIn, YouTube, Myspace, Hudl, Formspring, Instagram, Snapchat, GROUPME, WhatsApp, and blogs. A policy has been developed to protect you and the organization'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 express written authorization from a supervisor or administrator at the organization.

When using social media within written authorization through the organization 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 policy, no matter how small, can and will be subject to discipline as outlined fully in the employee handbook. You are personally responsible 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 organization on any non-organization-operated or sponsored site, you must state that:

"The views on this post are my own and not necessarily those of the organization."

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 organization, the organization's employees, vendors, clients, or other partners of the organization without written authorization.
- Do not use insults, obscenities, 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 at any organization-sponsored events.
- Respect all copyright, fair use, and financial disclosure laws.

Other Communications

Communications between organization personnel and students outside of the organization 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 personnel and minors 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"
- Communication through personal or non-organization-created 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.

Violations

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

I, _____, hereby certify and declare that I have read the Islamic Center of America's Information Technology Security Policy, I am certifying that I understand the Policy, and all the terms contained therein, and agree to abide by the terms and provisions contained within the Policy.

ISLAMIC CENTER
LET THE SUNNAH GO FORTH
Madrasatu Ahlis Sunnah
المَرْكَزُ الإِسْلاَمِيُّ لأَمْرِيكَا، مَدْرَسَةُ أَهْلِ السُّنَّة
AND DON'T STOP IT !!!
OF AMERICA