ISF Policy on
Information Technology Resource Access & Use

Policy

All information technology (IT) users must sign a document stating that they acknowledge having read, and agree to abide by, this policy.

Introduction

The Islamic Society of Frederick (ISF) provided access to information technology resources, including computers, networks, and peripheral devices, to support the ISF mission. The following guidelines apply to all who use and access ISF information technology resources.

Acceptable Use of ISF IT Resources

This section describes uses of ISF information technology systems that are considered acceptable by the ISF Board of Directors. The general criteria used in deciding acceptable use are whether the application is of benefit to ISF, whether it complies with government laws and regulations, and whether it does not adversely affect others. ISF allows the personal use of the Internet as long as it does not interfere with official business, increase cost to ISF, or embarrass ISF. Questions about the use of ISF information technology resources that are not explicitly mentioned in this policy should be directed to the ISF Board of Directors.

ISF information technology resources may be used in the conduct of ISF daily business, in the administration and management of ISF programs, and in the dissemination of information about ISF to the public. Examples of such use of ISF information technology include, but are not limited to:

- Management of ISF operations and staff;
- Maintenance of ISF web-based resources;
- Preparation of reports, memos, correspondence, databases, graphics, displays, and presentations;
- Use during ISF social events;
- Teaching classes in the ISF Sunday school or to the public.

ISF information technology resources may be used to communicate and exchange information with others located at ISF, and elsewhere, to share information related to the ISF mission. This includes other religious organizations, vendors and companies with products of interest to ISF, and the public. Examples of acceptable communication include, but are not limited to:

- Disseminating appropriate information related to ISF mission topics electronically;
- Communicating by electronic mail or other means for purposes of ISF business;
- Accessing public information available on the Internet, or elsewhere, related to the mission of ISF;
- Obtaining software patches, and updates from vendors, public domain software repositories, and other sources, provided such software is obtained, checked and tested, and installed in

accordance with U.S. copyright regulations, the license for that software, and ISF security policies;
- Participation in forums, news groups, and other information exchanges for the purpose of furthering the ISF mission or improving the professional knowledge or skills of ISF staff.

Software from the Internet and other public sources, and installing unnecessary software from any source, increases security risks to ISF networks and computers by potentially including things such as harmful viruses, back doors, and mechanisms specifically designed to defeat firewall protection. Users must follow the guidelines established by the ISF Board of Directors and the ISF IT-committee when downloading software from the Internet:

- Only install software that will be used for work-related functions.
- Only install or run software that was written by well-known, established sources. At a minimum, you should be able to identify the original source of the software and validate that you can locate and communicate with the author or company to discuss problems that might arise.
- Make sure antivirus software is installed, set to auto-protect, and maintained with current antivirus definitions before installing any software on ISF computers.
- Scan downloaded files for viruses before installing and running them. Generally "shrink-wrapped" commercial software should be free from viruses (although some manufacturers have distributed infected software).
- ISF software may be installed on non-ISF computers for work-related purposes (e.g. to work from home). ISF software must be removed from non-ISF computers when the IT user is no longer associated with ISF or when the IT user no longer needs the software for work-related purposes.

Acceptable Access to Information Technology Resources

ISF communications facilities may be used to provide access to ISF information technology systems and those of other organizations for authorized purposes. Examples of authorized access to systems include:

- Access to academic and government computer systems for accomplishing joint projects, where that access is authorized by the owner;
- Access to academic computing facilities for taking courses.

To ensure accountability of actions and resources, each person who has access to an ISF information technology system must have an individual account. Sharing of accounts and passwords or authorization methods is prohibited, except in special cases such as e-mail accounts for the operation of special services supported by a team of people.

Unacceptable Use of ISF Information Technology Resources

The use of ISF systems and networks in a manner which is unacceptable may subject the person(s) involved to loss of all privileges to use ISF systems, may result in other disciplinary sanctions up to and including dismissal, or may result in criminal prosecution. Unacceptable uses of ISF systems and networks include, but are not limited to:

- Commercial or business use for the profit of an individual, or company, or other use of ISF systems not approved by the ISF Board of Directors as essential to the ISF mission;
- Any use of ISF information technology resources in order to obtain access to any network or system at ISF, or elsewhere, for which the person has not been authorized, or in a manner that knowingly violates the policies of the owner of the network or system;
- Any activity that interferes with the legitimate activities of anyone using any ISF systems or networks, or any other network or system which may be accessed from ISF;
- Unauthorized use of a system for which the user has authorized access, including use of privileged commands on a system by a user not authorized to use such commands and unauthorized access to information owned by someone else. For example, no user may access the administrator account on a Microsoft Windows system or attempt to become an administrator on the system unless he or she is authorized to do so;
- Deliberate unauthorized destruction of ISF data or other resources;
- Any use of ISF information technology resources to engage in illegal or unethical activities;
- ISF expects users to conduct themselves professionally and to refrain from using ISF resources for activities that are offensive to coworkers or the public. Some examples include the use of ISF information technology resources that contain or promote (a) matters directed toward the success or failure of a political party, candidate for partisan political office, or partisan political group, (b) engaging in any action supportive of lobbying the Congress, (c) use of Internet sites that result in an unauthorized charge to ISF, (d) participating in prohibited activities such as discriminatory conduct, gambling, and disseminating chain letters, (e) intentional and unauthorized viewing of sexually explicit or pornographic material, (f) sending personal e-mail that might be construed by the recipient to be an official communication, (g) any activity that would bring discredit on ISF, (h) statements viewed as harassing others based on race, age, creed, religion, national origin, color, sex, handicap, or sexual orientation, (i) any violation of statute or regulation;
- The unauthorized sharing of ISF-owned software or any other ISF information not authorized for disclosure or use by others with anyone not specifically authorized to receive such software or information.
- Failure to follow ISF guidelines for downloading and installing software.

Privacy of Information

ISF systems and any information on those systems are ISF property. Therefore, users of ISF systems should be aware that information transmitted by or stored on ISF systems is not private. In addition, ISF users should also be aware that it is often necessary to monitor network traffic or computer activity to ensure integrity, security or reliable operation of ISF systems. However, any other monitoring is against ISF policy. Casual reading of e-mail messages addressed to others is prohibited.

Attachment to

ISF Policy on
Information Technology Resource Access & Use

I have read and understand the “ISF Policy on Information Technology Resource Access & Use” and agree to abide by this and all ISF IT security-related policies.

Name: (print clearly) ____
(First name, MI, Last name)

Signature: ____

Date: ____

ISF Board Member Name: ____

Signature: ____

Date: ____