Diocese of Saint Augustine Network Acceptable Use Policy
For All Parishes, Schools and Entities of the Diocese of Saint Augustine
Effective April 30, 2008

1.0 Glossary of Terms

1.1 Authorized users:

1. **"Employee":** Any lay person who is employed by or engaged in ministry in any Diocesan entity, whether part-time or full-time, who is given payment for services rendered, and for whom the diocesan entity is obligated to withhold payroll taxes (FICA, Medicare, and withholding).

2. **"Volunteer":** Any unpaid person engaged or involved in a diocesan activity, specifically as it relates to database creation and/or management, IT services, or internet-related services.

3. **"Church Personnel":** For purposes of this policy only, Church Personnel includes all individuals who minister, work, or volunteer in any school, parish, or ministry of the diocese whose compliance with this policy is sought. The term has no legal meaning or significance outside the scope of this policy and is not indicative of any employment or agency relationship.

4. **"Consultant":** Independent contractors, consultants, vendors or other persons who are not subject to the supervision of the Bishop of the Diocese of Saint Augustine and for whom no such duty to withhold payroll taxes exists, but provide expertise on database creation and/or management, IT services, or internet-related services.

1.2 Internet/Intranet/Extranet-related systems: include, but are not limited to, computer equipment, software, operating systems, storage media, network accounts providing electronic mail, World Wide Web browsing and FTP.

1. All internet/intranet/extranet-related systems are the property of the diocesan entity it serves. These systems are to be used for business purposes in serving the interests of the Diocesan entity, its staff and its constituents in the course of its normal operations.

1.3 Diocesan entity: Any parish, school, entity or ministry of the Diocese of Saint Augustine, including those entities which are separately incorporated under 501(c) (3).

1.4 Spam: Unauthorized and/or unsolicited electronic mass mailings.

1.5 IT: Information Technology

1.6 **Internet:** Includes both external and internal access of communications and data storage equipment, either owned or reserved for use by the diocese, by digital information devices including personal computers (PCs), personal digital assistants (PDAs) and similar devices. The term "Internet," as it applies to external resources, is meant to be all-inclusive and comprises other similar or analogous terms such as the "World Wide Web," "email," and "the Net."

1.7 **Network:** Communications system connecting two or more computers and their peripheral devices to exchange information and share resources. For the purpose of this policy this also includes stand alone computers.

2.0 Overview

The Diocese of Saint Augustine recognizes that the Network/Internet and other emerging technologies allow authorized users access to immense information globally. The Diocese of Saint Augustine's goal in providing this privilege to authorized users is to promote professional excellence, innovation and communication. The use of the Network/Internet or other emerging technologies will be guided by the Diocesan Network Acceptable Use Policy (DNAUP). All Diocese of Saint Augustine authorized users are required to sign a written DNAUP and to abide by the terms and conditions of the policy and its accompanying regulations.

3.0 Scope

This policy applies to authorized users of any school, parish or ministry of the Diocese of Saint Augustine, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or used by the diocesan entity.

4.0 Purpose

The purpose of this DNAUP is not to impose restrictions that are contrary to an established culture of openness, transparency, trust and integrity. Rather, the Diocese of Saint Augustine is committed to protecting its authorized users from illegal or damaging actions by individuals, either knowingly or unknowingly.

These rules are in place to protect authorized users and diocesan entities. Inappropriate use exposes Diocesan entities to risks including virus attacks, compromise of network systems and services and legal issues. Anyone with knowledge of inappropriate material/content should report this information verbally and in writing to the IT authority or the principal, pastor, or lay person in charge of the school, parish or ministry of the diocese.

5.0 Policy

5.1 General Use and Ownership

1. Authorized users should be aware that the data they create on systems remains the property of the Diocesan entity. Because of the need to protect the network, management cannot guarantee the confidentiality of information stored on any network device belonging to a Diocesan entity.

2. Authorized users are responsible for exercising good judgment regarding the use of network/computer systems. Authorized users should be guided by diocesan policies on personal use, and if there is any uncertainty, authorized users should consult their supervisor or manager.

3. The Diocese of Saint Augustine recommends that any information that users consider sensitive or vulnerable be encrypted, especially when stored on external media.

4. Authorized personnel, acting on behalf of the Diocese of Saint Augustine, may monitor equipment, systems and network traffic at any time. The Diocese of Saint Augustine maintains the right to monitor all network/computer activity derived from or utilized through its resources, whether it is online, downloaded or through printed material.

5. The Diocese of Saint Augustine, through its entities, reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

6. All data and files on network/computer systems are the property of the Diocese of Saint Augustine.

5.2 Security and Proprietary Information

1. Anyone responsible for entering information into a database or having access to database information used by any Diocesan entity, whether clergy, religious, employee or volunteer, must be FBI fingerprinted and background checked and cleared.

2. The appropriate IT authority of each Diocesan entity does everything possible to ensure the Diocesan entity network is properly maintained and adequate security measures are operational. To assist the appropriate IT authority of each Diocesan entity in sustaining this goal, authorized users, through their supervisor, should notify their IT authority when software and hardware modifications are necessary on any diocesan computer workstation. At no time should a computer be connected to a Diocesan entity network without the approval of the IT authority of the Diocesan entity.

3. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by school confidentiality guidelines. Staff and students should take all necessary steps to prevent unauthorized access to this information.

4. Passwords will be created by each authorized user for their own use, with the exception of students, volunteers and temporary/contractual personnel. Authorized user passwords shall not be shared. It is the responsibility of each authorized user to keep his/her password confidential. Anyone whose password becomes known to any other person should notify the IT authority immediately and a new password will be created. Anyone who becomes aware of anyone else's password should contact the IT authority immediately and a new password will be created. Temporary passwords used by students, volunteers or temporary/contractual personnel may be known by the supervisor and other appropriate authorities. However, temporary passwords should not be shared. System server level passwords should be changed quarterly by the IT authority; user level passwords should be changed every six months by user.

5. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (control-alt-delete for Windows 2000 Professional and above users) when the host will be unattended.

6. Due to the vulnerability of external media, such as flash drives, special care should be exercised to protect systems from damaging viruses in accordance to this policy. Authorized users are required to obtain supervisor approval before using, transmitting or taking files off-

site. Information considered sensitive and of a confidential nature, such as personnel files and payroll data, are not permitted to leave the work site for any reason.

7. Postings by authorized users from any diocesan email address to online bulletin boards, forums, chat rooms, web logs ("blogs")" and any other similar non-work-related discussion groups are prohibited, unless they are specifically work related.

8. All hosts used by the authorized user that are connected to any diocesan Internet/Intranet/Extranet shall be continually executing approved virus-scanning software with a current virus database.

9. Authorized users must use extreme caution when opening email attachments received from unknown senders, which may contain viruses, email bombs, or Trojan horse code.

10. Consult with your IT authority before sending "blast" emails. Sending email to more than 100 recipients at a time is considered a "blast" email. The diocese discourages this practice unless an outside vendor is used to manage the dissemination of such emails.

11. Whenever sending "blast" emails or emails to many recipients, use the blind copy (bc) for the recipients to ensure respect for the privacy of each individual address.

5.3 <u>Unacceptable Use</u>

1. A database of subscribers for parish or other diocesan entities can be a useful tool for parish or entity distribution of important messages, calendar of events, or other data. The marketplace is full of companies that offer such database opportunities. This type of database can also compromise a person's identity and/or place an individual in danger, if the database is misused, compromised or shared indiscreetly. No parish or Diocesan entity should create or subscribe to a vehicle by which subscribers, other than authorized personnel such as employees, priests, deacons, religious or those designated at the discretion of the pastor or head of the Diocesan entity, are given email addresses to communicate with other subscribers. This does not apply to instructional technology or methodology which includes approved subscriber access for a specific instructional purpose and is monitored for this purpose. This instructional technology should not offer chat or chat rooms separate from the monitored purpose. In addition, the application should NOT:

a. Allow blogs
b. Require or request photos of subscribers
c. Ask for age or gender of subscribers
d. Display subscriber email addresses
e. Allow subscribers access to other subscriber information

As we utilize the Internet, email and other technology for communication, we must be aware of serious and grave danger to our children and young people when information is misguided or given innocently to the wrong people.

2. The following activities are, in general, prohibited. Authorized users may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

a. Under no circumstances is an authorized user allowed to engage in any activity that is illegal under local, state, federal or international law while utilizing the Diocesan entity-owned resources.

b. Authorized users are prohibited from attempting to circumvent or subvert any system's security measures. Authorized users are prohibited from using any computer program or device to intercept or decode passwords or similar access control information.

c. When an authorized user becomes "unauthorized" by virtue of employment, dismissal, graduation, retirement, etc., or if the authorized user is assigned a new position and/or responsibilities within the diocesan system, his/her access authorization will automatically be reviewed with the appropriate individual to determine whether continued access is warranted. This person may not use facilities, accounts, access codes, privileges or information for which he/she has not been authorized.

d. **System and Network Activities:** The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the Diocesan entity.

2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the Diocesan entity or the end user does not have an active license is strictly prohibited. Public disclosure of information about programs (e.g. source code) without the owner's authorization is prohibited.

3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, email bombs, etc.).

5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

6. The installation or use of Instant Messaging is prohibited.

7. Using a diocesan computing asset to access inappropriate or offensive material or to engage in the procuring or transmitting of material that violates Diocesan anti-harassment or hostile environment policies.

8. Making fraudulent offers of products, items or services originating from any Diocesan entity account.

9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the authorized user is not an intended recipient or logging into a server or account that the authorized user is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, 'disruption' includes, but is not limited to, creating or propagating viruses, hacking, network sniffing, spamming, pinged floods, packet spoofing, password grabbing, disk scavenging, denial of service and forged routing information for malicious purposes.

11. Port scanning or security scanning is expressly prohibited unless prior notification is made to the Diocese of Saint Augustine.

12. Executing any form of network monitoring which will intercept data not intended for the authorized user's host, unless this activity is a part of the authorized user's normal job duty.

13. Circumventing user authentication or security of any host, network or account.

14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

15. Posting photos, digital video, and other personal information of children and diocesan personnel, without authorization, to Internet sites is prohibited. This includes, but is not limited to, activities that are conducted on personal computer equipment off-site and after working hours.

16. Peer-to-Peer file sharing. This includes, but is not limited to, Lime wire, Morpheus and Napstar.

e. Employee Responsibilities:

i. Privacy: No authorized user should view, copy, alter or destroy another's personal electronic files without permission.

ii. Harassment, Libel and Slander: Under no circumstances, may any authorized user use Diocese of Saint Augustine computers or network resources to libel, slander or harass any other person.

iii. Abuse of Computer Resources: Abuse of Diocese of Saint Augustine computer resources is prohibited. This abuse includes, but is not limited to, the following:

1. Unauthorized use of software: Software downloaded from the Internet or loaded from disks and flash drives is prohibited unless approved by the IT authority.

2. Game Playing: Installing or playing recreational games, which is not part of authorized and assigned job-related activity, are considered unacceptable practices and are prohibited.

3. Chain Letters: The propagation of chain letters (email), “Ponzi” or other “pyramid” schemes of any type are considered an unacceptable practice and are prohibited.

4. Unauthorized Servers: The establishment of a background process that services incoming requests from anonymous diocesan employees for purposes of music/radio/video continuous Internet connectivity, chatting or browsing the Internet is prohibited.

5. Unauthorized Monitoring: An employee may not use computing resources for unauthorized monitoring of electronic communications of other employees.

6. Private Commercial Purposes: Personal use of network and computer resources of the Diocese of Saint Augustine is prohibited.

5.4 **Email and Communications Activities:** Diocesan entities maintain electronic mail systems. These systems are provided by the Diocesan entity to assist in conducting business within the diocese.

1. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages is not allowed.

2. Unauthorized use, or forging, of email header information is not allowed.

3. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies is not allowed.

4. Posting the same or similar non-business-related messages to large numbers of newsgroups (newsgroup spam) is not allowed.

5. The electronic mail system hardware is the property of the Diocesan entity. Additionally, all messages composed, sent or received on the electronic mail system are and remain the property of the Diocesan entity. The diocese, through the appropriate authority, reserves the right to review, audit, intercept, and access all messages created, received or sent over the electronic mail system for any purpose.

6. The email system was created to facilitate operations of the Diocesan entity. It should be used primarily for business purposes, and only incidentally for personal use. Likewise, personal email through such networks as AOL, Yahoo, Gmail, and others should be accessed on a limited basis, unless those networks are being used for diocesan business.

7. The electronic mail system may not be used to solicit or proselytize for commercial ventures, political causes, outside organizations or other non-job related solicitations.

8. The electronic mail system is not to be used to create any offensive or disruptive messages. Among those which are considered offensive are any messages which contain sexual implications, racial slurs, gender-specific comments, or any other comment that offensively addresses someone’s age, sexual orientation, religious or political beliefs, national origin, disability, veteran or marital status.

9. The confidentiality of any message should not be assumed. Even when a message is erased, it is still possible to retrieve and read that message. Further, the use of passwords for security does not guarantee confidentiality.

10. Notwithstanding the diocese's right to retrieve and read any electronic mail messages, such messages should be treated as confidential by other authorized users and accessed only by the intended recipient. Authorized users are not authorized to retrieve or read any email messages that are not sent to them.

11. Authorized users shall not use a code, access a file, or retrieve any stored information, unless authorized to do so. Authorized users should not attempt to gain access to another authorized user's messages without the latter's permission.

12. All authorized users should perform routine maintenance of their mailboxes and delete messages they are no longer using.

13. The appropriate authority should be notified if a user becomes aware of emails which violate this policy.

14. Extreme care should be exercised when sending emails with sensitive information due to the fact that a majority of email systems are not encrypted and secure.

6.0 Enforcement

Effective security is a team effort involving the participation and support of every authorized user who deals with information and/or information systems. It is the responsibility of every authorized user to know these guidelines, and to conduct their activities accordingly. The Diocese of Saint Augustine does not sanction any use of the Network/Internet and other available technology that is not authorized by or conducted strictly in compliance with this policy and its regulations. Authorized users who disregard the DNAUP may have their Network/Internet privileges suspended or revoked and may be subject to appropriate corrective action, up to and including termination. The Diocese of Saint Augustine reserves the right to suspend or revoke such privileges in the event that any supervisor believes the authorized user's conduct to be inappropriate or noncompliant with the DNAUP. Authorized users granted access to the Network/Internet and other technologies through the Diocese of Saint Augustine assume personal responsibility and liability, for their actions. In addition, any employee, volunteer, or contractor found to have violated this policy may be subject to corrective action, up to and including termination. Authorized users who have read and signed the DNAUP form and who agree to act in a considerate and responsible manner will be authorized Network/Internet access.

7.0 System Back-up(s)

Although system back-ups should be provided by the Diocesan entity as standard operating procedure, it is the responsibility of each authorized user to backup his/her specific computer workstation data. Depending upon the amount of the individual workstation usage, workstation backups should occur daily.

8.0 Virus Protection

All networked computers must have current virus protection software, operating system updates, such as Windows updates, installed and operational at all times. Windows updates should occur at least monthly.

9.0 **Website Requirements**

Diocesan entity websites are not permitted to link to other websites that are in conflict with church teaching and the Magisterium of the Roman Catholic Church. Permissible links fall into these main areas:

1. Official Church sites, such as the Vatican, United States Conference of Catholic Bishops, state conferences, archdioceses and dioceses;

2. Parts of the diocese such as parishes, schools and ministries operated by the diocese or approved resources associated with those ministries; and

3. Under the oversight of a bishop or religious congregation, or listed in the Official Catholic Directory. Church leaders should use prudence in evaluating links to other commercial opportunities on its site. It is the diocesan entity's responsibility to evaluate its hosts' advertisers and sponsors on a regular basis.

4. Use of photos on websites should be group photos. Where children are involved, first names only should be used. Parents/guardians must sign permission slips each year for use of children's photos; therefore, all photos, particularly those which include children, should be refreshed regularly.

5. Approved websites by Diocesan entities should post the following disclaimer to the homepage of each site:

   "Although links to and from this website are monitored frequently for content, anyone who finds inappropriate content should immediately notify the [Diocesan entity] so the link may be reviewed and/or removed."

6. All diocesan parishes, schools and entities should have a link to the Diocese of Saint Augustine website, www.dosafl.com, on its own website.

7. Diocesan entities, with the exception of parishes and schools, must obtain approval from their supervisor and/or Director of Communications before establishing a website.

10. In order to provide interactive service, Diocesan entities may collect personally-identifiable information from the users of the website. If such information is collected, the user will be informed about this practice. Additionally, if a website is directed to children or if a general audience website collects personal information from children, the Diocesan entity must comply with the Diocese of Saint Augustine online privacy policy. The privacy policy is attached and also posted on the Diocese of Saint Augustine website under policies and procedures at www.dosafl.com.

As a condition to use the Diocesan Network/Internet, I agree to abide by the terms and conditions of DNAUP, and I understand that my access may be suspended or terminated if I violate the policy.

Signed: _____
Name

Printed Name: _____

Date: _____

Position: _____

Parish/Entity: _____

Best Practices

Computer Security and Virus Protection:

- Install anti-virus software and keep it up-to-date
- Be cautious when opening email attachments

Spyware

Spyware installs itself onto a user's computer by stealth, subterfuge and/or social engineering and sends information from that computer to a third party without the user's permission or knowledge. Spyware includes keyloggers, backdoor Trojans, password stealers, and botnet worms, which cause corporate data theft, financial loss and network damage. To protect your computers against it, the computers utilizing your network need to have a spyware detection program. Good anti-virus programs can detect and remove spyware programs, which are treated as a type of Trojan.

Spam Filters

Follow these guidelines to help lower your risk of getting junk email:

- Take advantage of the Junk Email Filter in Outlook 2003 or 2007
- Increase your protection level as you need to High or to Safe Lists Only.
- Keep your Junk Email Filter updated
- Block images in HTML messages that spammers use as Web beacons
- Don't forward chain email messages
- Don't contribute to a charity based on a request in email
- If a company uses email messages to ask for personal information, don't respond by sending a message
- Don't reply to spam
- Watch out for checked boxes that are already selected when you buy things online
- Review the privacy policies of websites
- Use multiple email addresses for different purposes
- Disguise (or "munge") your email address when you post it to a newsgroup, chat room, bulletin board, or other public places
- Limit where you post your email address
- Anti-spam software should be installed with the email server.

Content Filters

- Content filtering is the blocking of content based on a rating system that is static, dynamic or a combination of both. Several content filtering products use a remote database of previously classified sites or IP addresses in conjunction with a local cache of frequently or recently requested sites. Some use a dynamic rating system that evaluates the content on the fly. Newer dynamic rating technologies offer more protection and use context-based rules instead of relying only on single keyword blocking.
- All content filtering products will have about a dozen different content categories, such as Violence, Pornography, Hate/Racism, Nudity, and so on.
- Some content filter manufacturers you may be familiar with include SonicWall, WatchGuard, Websense, Surfcontrol and Symantec. These products offer gateway control; there are numerous client-based products available that load on the desktop, but capabilities are limited and management is difficult for a network with even a handful of PCs.

System Backup

- Develop backup and restore strategies and test them. With a good plan, you can quickly recover your data if it is lost.
- Back up all data on the system and boot volumes and the System State. This precaution prepares you for the unlikely event of a disk failure.
- Create an Automated System Recovery (ASR) backup set when the operating system changes, for example, whenever you install new hardware and drivers or apply a service pack. With an ASR backup set, you can more easily recover from a system failure. Also, backup all data volumes at the same time; ASR protects only the system, so data volumes must be backed up separately.
- Create a backup log. Keep a book of logs to make it easier to locate specific files.
- Retain copies. Keep at least three copies of the media. Keep at least one copy off-site in a properly-controlled environment.
- Perform trial restorations to verify that your files were properly backed up. A trial restoration can uncover hardware problems that do not show up when you verify software.
- Secure devices and media. It is possible for someone to access the data from a stolen medium by restoring the data to another server for which they are an administrator.

Secure Network Closets

When designing and building telecommunications closets make sure that they are:

- At least One Closet Per Floor
- A safe working environment
- Provide enough space for today's technology as well as potential for scalability.
- Minimum telecommunications closet size
- Include space for an uninterruptible power supply in each closet. There should be a minimum of two electrical circuits in each closet. Design for good even lighting throughout the entire closet space both high and low. And finally provide for enough cooling capacity for the electronics in the room.
- Make sure there is some access control and they are not open to the public.

Password Policy

All computers, laptops, workstations and servers should be secured with a password protected screensaver with the automatic feature set at 10 minutes or less, by logging off or locking the station when it will be unattended.

Passwords must meet the following minimum requirements when they are changed or created:

- Not contain significant portions of the user's account name or full name
- Be at least six characters in length
- Contain characters from three of the following four categories:
    - English uppercase characters (A through Z)
    - English lowercase characters (a through z)
    - Base 10 digits (0 through 9)
    - Non-alphabetic characters (for example, !, $, #, %)

Define the maximum password age policy setting so that passwords expire as often as necessary for your environment, typically, every 30 to 90 days.