Diocesan Network Acceptable Use Policy

1.0 Overview

The Diocese of Orlando recognizes that the Network/Internet and other emerging technologies allow authorized users access to immense information globally. The Diocese of Orlando'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 Orlando authorized users are required to sign a written DNAUP and to abide by the terms and conditions of the policy and its accompanying regulations.

2.0 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 Orlando 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 specialist or the principal, pastor, or lay person in charge of the school, parish or ministry of the Diocese.

3.0 Policy

3.1 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 reasonableness of personal use. 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 Orlando recommends that any information that users consider sensitive or vulnerable be encrypted, especially when stored on external media.

4. Authorized personnel may monitor equipment, systems and network traffic at any time. The Diocese of Orlando maintains the right to monitor all network/computer activity

derived from or utilized through its resources, whether it is on-line, down-loaded or through printed material.

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

6. Authorized users are advised that a determined individual may be able to gain access to services on the Network/Internet and other technologies which the Diocese of Orlando has not authorized for professional purposes. By participating in the use of the Network/Internet or other technologies, authorized users may gain access to information and communications which the authorized user may find inappropriate, offensive or controversial. Authorized users assume this risk by consenting to the use of the Network/Internet with the Diocese of Orlando.

7. Anyone who removes diocesan equipment from the business location is required to sign the Receipt of Computer Equipment form. This would include employees who require equipment while working away from the office. If equipment is removed for repair the Receipt of Computer Equipment form or appropriate receipt from vendor can be used.

3.2 Security and Proprietary Information

1. Anyone responsible for entering information into a database or have 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 knowledge of the IT authority of the Diocesan entity.

   At no time should a computer be connected to a Diocesan entity network without the advanced knowledge and approval of that Diocesan entity's recognized IT authority. Connecting computers and peripheral devices not owned by the Diocese of Orlando (unauthorized devices) to a Diocesan entity network is prohibited unless approved in advance. This includes, but is not limited to, personal computers, printers, flash drives or other external storage devices, switches, routers and wireless equipment. Requests to connect unauthorized devices will be evaluated on a case by case basis.

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.

3. Passwords will be created by each authorized users 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 appropriate authority immediately and a new password will be created. Anyone who becomes aware of anyone else's password should contact the appropriate authority immediately and a new password will be created. Temporary passwords used by students, volunteers or temporary/contractual personnel may be known by the appropriate authority. However, temporary passwords should not be shared. System passwords should be changed quarterly; user level passwords should be changed every six months.

4. 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 Win2K users) when the host will be unattended.

5. Because information contained on external media is especially vulnerable, special care should be exercised to protect it in accordance to this policy.

6. Postings by authorized users from any Diocesan email address to on-line bulletin boards, forums, chat rooms, web logs ("blogs")" and any other similar non-work-related discussion groups is prohibited, unless it is specifically work related.

7. 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.

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

9. Whenever sending "blast" e-mails or e-mails to many recipients, use the blind copy (bc) for the recipients to ensure respecting the privacy of each individual address.

3.3 Unacceptable Use

1. A database of subscribers for parish or other Diocesan use can be a useful tool for parish or Diocesan entity distribution of important messages, calendar of events, or other data. The marketplace is full of companies which 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 mis-used or shared indiscreetly. No 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 Diocesan entity head, are given e-mail 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 without the written and express permission of each subscriber of the database:

- **a.** Offer Chat or Chat Rooms
- **b.** Allow Blogs
- **c.** Require or Request Photos of Subscriber
- **d.** Require or Request Video of Subscriber
- **e.** Ask for Age or Gender of Subscriber
- **f.** Display Subscriber E-Mail Addresses
- **g.** Allow Subscribers Access to Other Subscriber Information

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, e-mail 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 to Diocese of Orlando is made.

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.

e. Employee Responsibilities:

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

2. Harassment, Libel and Slander: Under no circumstances, may any authorized user use Diocese of Orlando computers or networks resources to libel, slander, or harass any other person.

3. Abuse of Computer Resources: Abuse of Diocese of Orlando computer resources are prohibited. This abuse includes, but is not limited to, the following:

a. 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 during normal work hours.

b. Chain Letters: The propagation of chain letters (e-mail), "Ponzi" or other "pyramid" schemes of any type are considered an unacceptable practice and are prohibited.

c. 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.

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

e. Private Commercial Purposes: The computing resources of Diocese of Orlando shall not be used for personal or private commercial purposes or for financial gain.

3.4 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 e-mail 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 e-mail through such networks as AOL, Yahoo, Gmail, should be accessed on a limited basis.

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 or disability.

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 e-mail 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 e-mails which violate this policy.

14. When communicating to a minor through any correspondence such as regular mail, e-mail, text or other technological opportunities for correspondence, such as educational programs, etc., the correspondence must be accompanied by a corresponding copy to the parent.

15. It is the responsibility of the minister or entity to collect parent e-mail addresses and monitor correspondence to be sure parents receive notification at the same time a minor notification is sent.

16. All correspondence must be professional in nature and appropriate for the ministry from which it was sent.

17. Each Diocesan Entity must have a registered domain name that provides appropriate identification of the entity. The preferable Top Level Domain (TLD) is ".org" which is appropriate for nonprofit organizations. All domain names must be registered in the name of the Diocesan entity and not be registered in the name of an individual. Domain registrations can be set to "auto-renew" with the registrar. The auto-renew feature will help prevent domains from expiring unintentionally.

18. Business email accounts must only be provided to approved employees. The creation of business email accounts for employees must be approved in writing by the Pastor or Administrator. Temporary employees and interns can be issued an email account that uses the official domain but the email address should be generic in nature and should not identify the person by name. (e.g., receptionist@orlandodiocese.org, intern@orlandodiocese.org, etc.)

19. Business email accounts must use the domain referred to in the paragraph above. Business email should not use generic domains such as yahoo.com, gmail.com, hotmail.com, etc.

4.0 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.

5.0 Virus Protection

All networked computers must have current virus protection software installed and operational at all times.

6.0 How to Comply With The Children's Online Privacy Protection Rule

In order to provide interactive service, Diocesan entities might collect personally-identifiable information from the users 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 Orlando on-line privacy policy. The privacy policy is posted on the Diocese of Orlando website, www.orlandodiocese.org.