

Diocese of Orlando
Network Acceptable Use Policy
for All Parishes, Schools and Entities of the Diocese of Orlando
Parent Addendum

5.3 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 database should NOT:
 - a. Offer Chat or Chat Rooms
 - b. Allow Blogs
 - c. Require or Request Photos of Subscriber
 - d. Ask for Age or Gender of Subscriber
 - e. Display Subscriber E-Mail Addresses
 - f. 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.

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 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.

10.0 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, http://www.orlandodiocese.org/outreach/child_youth/online_policy.html.

I agree to abide by the terms and conditions of the Parent Addendum of DNAUP.

Signed _____
(*Name*)

Printed Name: _____

Date: _____

Position: _____

School: _____

E-mail address: _____