

## ATTACHMENT A

### **Section 408: Policy for the Use of the Internet, Electronic Communications and Other Technology**

#### 1. **Introduction**

The purpose of this Policy for the use of the Internet, Electronic Communications and Other Technology (the "Policy") is to give users of the Catholic Diocese of Cleveland's (the "Diocese") electronic communication systems clear guidance on what can and cannot be done with such systems. Failure to follow this Policy can result in violations of the law, costly fines and penalties, expensive lawsuits and judgments, and otherwise impair the Diocese's ability to conduct its affairs; therefore, it is critical to strictly follow this Policy.

#### 2. **Scope of Policy**

Electronic communications include, but are not limited to, electronic mail, instant messaging, access to and use of the Internet, Diocese-run networks and websites, network services, facsimile (fax), file transfers, electronic data interchange, audio and video teleconferencing, voice mail, telephone systems and wireless technologies such as personal digital assistants (PDA's), cellular phones and pagers.

"Electronic communication system" or "System" as referred to in this policy is any system which is necessary or desirable to support the Diocese electronic communications, which is owned, leased or otherwise contracted for by the Diocese, or which is being used to access the Diocese's electronic communications or otherwise being used in furtherance of the Diocese's business, whether or not owned or leased by the Diocese, including such equipment that is owned or leased by an individual user.

This Policy applies to all employees, representatives and agents of the Diocese and any other users of the Electronic Communication System (collectively referred to as "Users").

The effective date of this Policy is January 1, 2003, superseding prior policies. Any and all amendments or changes to this Policy must be approved in advance by the Legal Office of the Diocese. Final interpretation of this Policy shall be by the Legal Office of the Diocese of Cleveland.

The Diocese reserves the right, solely at its discretion, to change this Policy at any time with such notice as the Diocese deems appropriate. Individual parishes, schools, or other entities may, at their discretion, enforce stricter rules than what is stated in this policy and guidelines.

#### 3. **General**

3.1 **Intended Use.** The Electronic Communication System is intended primarily for use in connection with the Diocese's mission and related services.

3.2 **No Expectation of Privacy.** Communications created, sent, received, stored and/or accessed using the Electronic Communication System are not private. It is not the intention of the Diocese to regularly monitor the content of User's electronic communications. The Diocese reserves the right, however, to monitor, review, electronically scan, audit, intercept, access and disclose all electronic communications and data that are created, sent, received, stored and/or accessed using the Electronic Communication Systems, to support operational, maintenance, quality, auditing, security, and investigative activities and to ensure compliance with this Policy, the Diocese's Personnel Practices Manual, the Policy Regarding Allegations of Child Abuse or otherwise to further the Diocese's mission. The Diocese may also disclose the contents of a User's electronic communications or data to third parties without prior notice to or consent of the User. The Diocese will also respond to legal process, complaints or use in violation of this Policy and fulfill its obligations to third parties. For that reason, Users do not have the same expectation of privacy in their use of the Electronic Communication System as with personally-owned, non-Electronic Communication System, communication tools. Users should not expect privacy, and Users should structure their electronic communications in recognition of the fact that the Diocese may from time to time examine the content of electronic communications. Moreover, the deletion of a message or document may not fully eliminate such message or document from the Diocese computer network. All Users waive any right to privacy in their use of the Electronic Communication System and consent to access and disclosure of such documents/messages by authorized Diocese personnel.

3.3 **Ownership.** All electronic communications and data that are created, sent, received, stored and/or accessed using the Electronic Communication Systems are Diocese property. All data and information created, sent, received, stored and/or accessed by employees of the Diocese during their employment by the Diocese, and which relates in any way to their employment by the Diocese, is the property of the Diocese, whether such data is stored or accessed using the Electronic Communication Systems, maintained in hard copy, or stored electronically on systems not belonging to the Diocese. Moreover, all hardware, infrastructure and software provided by the Diocese is owned by the Diocese. Users are responsible for maintaining such property in good condition and shall return such property to the Diocese upon termination of its use or upgrade.

#### 4. **Security Obligations**

The goal of information system security is to protect information from unauthorized or inappropriate access or modification. The Diocese will maintain a system of information security to protect its proprietary data. An integral part of this system is the policies, standards and procedures set forth below. All Users must adhere to these policies, standards and procedures for the Electronic Communication System to remain viable and should immediately report any suspected, attempted or actual security violations or breaches.

4.1 **Safeguards.** Users must take appropriate care to safeguard the security and integrity of the Electronic Communication System and not deliberately interfere with the Diocese's access to data stored on the System or deliberately circumvent the Diocese's security procedures. Users should not add additional security, such as passwords, to their workstations or files.

4.2 **Unauthorized Access.** Users are prohibited from using the System in any manner that creates an unreasonable risk of permitting unauthorized outside access to the Electronic Communication System. Persons who are not authorized Users may not be given access to, and are not permitted to use, the Electronic Communication System unless such access or use has been approved in advance by the Diocesan Human Resources Department. If approved, then those persons (including contractors and temporary employees) are subject to this Policy.

4.3 **User Identification and Passwords.** Users shall not share centrally-administered passwords. In an emergency or unusual situations, sharing of passwords for applications with a trusted coworker is permitted. Questions about sharing passwords should be directed to your Technical Support Representative. Users must inform their Supervisor and Technical Support Representative of any password necessary to obtain access to any security or "lock down" application (such as screen savers, BIOS passwords, etc.) when they are absent while their computer or application requires repair or maintenance.

4.4 **Accurate Identification.** Users shall identify themselves to the system by signing on with their assigned user name. Users shall not misrepresent, obscure, suppress or replace a user's identity on an Electronic Communication System. The user name, electronic mail address, Instant Messenger ("IM") mail address organizational affiliation and related information included with electronic messages or postings must reflect the actual originator of the messages or postings.

4.5 **Viruses.** Since viruses are often transmitted through e-mail attachments, before attaching an attachment, Users should verify through the use of approved anti-virus software that the attachment does not contain any viruses (such anti-virus software must be installed and kept active at all times on all computers used in connection with the System). Also, when accessing an attachment, Users should always save the attached document to disk or the hard drive, rather than opening it directly. While some file attachments are just web pages or external text files, others are programs, some of which may contain viruses. Be particularly careful with any files that have ".exe", ".vbs.", ".scr" extensions, especially when receiving file attachments from unknown sources. Before downloading and opening any file from the Internet, the User should scan the file for viruses. The same precautions should be taken with respect to diskettes.

4.6 **Connection to the Internet.** Users shall use the Electronic Communication System in a manner that does not compromise the security and integrity of the Diocese's network, such as allowing intruders or viruses into the Diocese's network. When using any computer attached to the Diocese's network, users shall not access the Internet except

through a Diocese-approved Internet firewall. Users shall not access the Internet directly, whether through a modem or otherwise, unless the accessing computer is disconnected from the Diocese's network.

4.7 **Instant Messaging.** Information sent using instant messaging (for example, AOL Instant Messenger™) is analogous to sending a postcard -- the information cannot be encrypted and is easily intercepted-- and as such is not secure. If a User accesses an instant messaging service using the System, the User shall select and use a user name that corresponds to their Diocese-assigned e-mail address and shall obtain their Supervisor's approval.

4.8 **Breach.** Any security breach, substantiated or not, must be reported to the Technical Support Representative.

## 5. **Confidentiality**

5.1 **No Dissemination.** Use of the System to disseminate the Diocese's confidential information outside the Diocese is expressly prohibited. Special care should be taken when forwarding e-mail messages, especially instant messages. Confidential or proprietary Diocese information must not be forwarded to any party outside the Diocese without the prior approval of the employee's direct supervisor and the Secretary or equivalent level department head and the information's owner/originator. A secure messaging system and a confidentiality header must be used in these circumstances. For Example, "CONFIDENTIAL – This message and any attachments are confidential, and intended only for the individual or entity named above. If you are not the intended recipient, please do not read, copy, use or disclose this communication to others; also please notify the sender by replying to this message, and then delete it from your system. Thank you." Blanket forwarding of messages to parties outside the Diocese is prohibited.

5.2 **No Interception.** Users shall not intercept or disclose, or assist in intercepting or disclosing, electronic communications unless specifically authorized by the Diocese.

5.3 **Cellular Phones.** Confidential or sensitive information should not be communicated using a cellular telephone, as it may not be a secure method of transmission. Additionally, it is against Diocese policy to conduct Diocese business by phone or other electronic devices while operating a motor vehicle.

5.4 **Employment Agreement Obligations.** This Policy does not alter or change an employee's obligations to the Diocese under their Employee Agreement concerning confidential information.

5.5 **Confidential Information Defined.** Confidential Information includes all information that is not generally available to the public, including, without limitation, financial information, personnel files, personal information provided by members of the church, or any other information that may be deemed as confidential.

## 6. Content of Messages

Users of the Electronic Communication System are expected to use common sense and good judgment, taking into account that the very nature of such systems allow for messages to be forwarded quickly and accidentally to the wrong person. It is particularly important that Users apply this practice in what they say in the content of their electronic messages and in their access of the Internet. *Assume that your message may be accessed, forwarded and read or heard by someone other than the intended recipient -- even if it is marked as "private"*. Also, Users should not intentionally access any site that is inappropriate for the Diocese, or which could cause embarrassment to the organization or the User. While not every standard can be listed here, the following are some common examples to guide your use of the System:

6.1 **Confidential Information.** Electronic communications should not contain sensitive, critical, confidential or proprietary information, unless encrypted or otherwise secured according to standards established by the Diocese, and even then, limited only to necessary recipients - refer to Sections 4 and 5, above.

6.2 **Acts that might create a "hostile environment".** Use of the System in a way that violates the Diocese's Uniform Code of Personnel Practices, including but not limited to sections 401 and 402; or to disseminate or intentionally access material that is defamatory, sexually oriented, obscene, pornographic, harassing, threatening, illegal, fraudulent, offensive or unwelcome to coworkers is expressly prohibited. In the event that accessing such materials is directly relevant and required by the User's work, the User shall get, in writing, a waiver for access, approved by his/her direct supervisor and the Secretary or equivalent level department head. Such waiver will have an expiration date not to exceed one year.

6.3 **Unauthorized use or copying of software, copyrighted materials or of information belonging to others.** Use of the System for unauthorized copying of copyrighted software or content is expressly prohibited. Similarly, proprietary information belonging to others must not be placed on the System without the prior written approval of the Director of Communications.

If a User receives notice, in writing or otherwise, or becomes aware that the Electronic Communication System is being or is proposed to be used to create, disseminate, store, upload or download any messages, communications or other material in violation of the copyrights, trademarks, patents, intellectual property or other property rights of any party, such User shall inform the Diocese in writing of such use or proposed use. The Diocese has designated the Diocesan Legal Office to receive notification of claimed infringement. The Diocese reserves the right to remove or disable access to any material that is claimed to be infringing or to be the subject matter of infringing activity.

6.4 **Illegal export.** The U.S. and some other countries prohibit the transfer of certain technical data without an export license. No such transfers should be done through the Electronic Communication System without proper approval.

6.5 **Privacy.** The Diocese has a Privacy Policy, as found on the Diocesan website, and certain national and local governments may have privacy laws, which may restrict the use or transmission of personally identifiable data. Check with the Diocesan Legal Office for these restrictions and laws.

6.6 **Unauthorized announcements and solicitations.** The System may not be used for political or social announcements not directly connected with the Diocese unless such announcements are placed in areas specifically designated for that purpose or prior approval by the Diocese has been obtained. Questions may be directed to the Director of Communications and Media Relations.

6.7 **Bulk E-Mail.** The System may not be used to send unsolicited advertising, junk, or chain e-mail messages (also known as “spam”). When sending out bulk e-mail (where one message is sent to numerous recipients):

- ensure that all recipients have requested to receive such communications from the Diocese (for example, by filling out a registration form);

- follow e-mail service provider’s policies or terms and conditions;

- label advertisements with “ADV” in the subject line;

- ensure that all information in the text and header are accurate, including the e-mail’s point of origin;

- ensure that the e-mail is sent with proper routing and transmission;

- use the “bcc” field rather than the “to” or “cc” fields to list recipients’ e-mail addresses;

- include in the body of the message the sender’s name, address and e-mail address and clear and conspicuous instructions for how to request to be removed from the mailing list and remove all recipients who have opted out from all mailing lists used by the Diocese; and

- send a copy of all such e-mail messages to the Secretary of your Secretariat and the Director of Communications and Media Relations.

Unsolicited electronic mail or communications received from unknown sources should be promptly discarded without forwarding to anyone and/or without responding in any manner to the originator.

6.8 **Attachments.** All file attachments to e-mail messages should be under **one megabyte** in size.

## 7. **Additional User Obligations**

7.1 **Back-ups.** In order to conserve limited resources, files that are not Diocese-related should not be stored on the Diocese's network servers. The Diocese has no responsibility to provide copies of personal data to employees leaving the Diocese.

7.2 **Access of Diocese Facilities by Non-Diocese-Provided Equipment.** Access to the Diocese's internal computer networks using non-Diocese-provided computers or PDAs, including access from remote locations such as employee homes, hotel rooms and affiliates, must in all instances be approved in advance by each individual Secretariat or other Business Unit. Such remote access may be revoked at any time for any reason, including failure to comply with the Diocese's security policies.

7.3 **Publication.** Users placing information on the Internet relating to the Diocese or in the course of performing his/her employment duties are, in effect, publishing such information on the Diocese's behalf. Only authorized personnel shall engage in such publishing activities, other than the sending or receiving of e-mail. Authorized personnel shall observe all existing standards, policies and regulations regarding materials published on the Diocese's behalf, and shall establish accountability for all information regarding the Diocese's mission or publications posted on the Internet for public access, including postings on electronic bulletin boards, chat rooms and information obtained "hyperlinks" to externally stored information. In no event shall a User represent his or her personal opinions as those of the Diocese or misrepresent oneself as another individual, church, parish or company. No materials are to be placed on the Diocese website without the approval of the Users Secretary or other head of the Users employing entity. No new websites shall be developed without the prior written approval of the Communications Director.

7.4 **Limited Personal Use.** The Diocese permits the occasional personal use of the Electronic Communication System by Users, however, Users should understand that personal use (a) must not in any way interfere with or impede the Diocese's mission, (b) must be occasional and minor, (c) must be promptly discontinued at the request of the Diocese, and (d) is expressly subject to all of the provisions in this Policy, as well as all other applicable Diocese policies and guidelines.

7.5 **"Recreational" Use.** Use of the systems for "recreational" uses (non-business Internet access, games, music, talk radio stations, etc.) is prohibited when engaging in such activity interferes with an employee's job duties, violates the Diocese's Uniform Code of Personnel Practices, or interferes with the efficient functioning of the System.

7.6 **Software.** All software used in connection with the System must be authorized by, or acquired through, the Diocese. The Diocese complies with all software copyrights and the terms of all software licenses. Users may not duplicate licensed software or related documentation or download such material unless the license agreement expressly allows for such use and the Diocese approves. The Diocese

reserves the right to remove any unauthorized software from any Diocese or parish-owned equipment or any personally-owned equipment on the Diocese premises. The Diocese reserves the right to conduct audits of the System to ensure that the Diocese and its Users are in compliance with all applicable software licenses and internal policies. Users are expressly prohibited from downloading or transmitting unauthorized or unlicensed software from the Internet or other sources onto the System. The downloading of “freeware” or “shareware” from the Internet is also prohibited unless approved by the Technical Support Representative of the User’s operating unit.

7.7           **Use of Credit Cards.** Diocese-issued credit cards shall not be used for any purpose to conduct transactions on the Internet without the prior written approval of the User’s Secretary or equivalent departmental head. Any such use must be kept on file with the User’s Secretary or equivalent departmental head and copied to the Finance Office.

## 8.           **Violations**

8.1           Violations of this Policy may lead to discipline up to and including termination of employment with the Diocese.