



**COMPUTER POLICIES AND PROCEDURES
FOR THE
ARCHDIOCESE OF DETROIT**

TABLE OF CONTENTS
STATEMENT OF PURPOSE
INTRODUCTION
STANDARDS FOR UTILIZATION OF ELECTRONIC MEDIA
BASIC POLICY
PROCEDURES
SECURITY
BASIC POLICY
PROCEDURES
USER AGREEMENT FORM

STATEMENT OF PURPOSE:

With Jesus, the Great Communicator, and in the spirit of our Christian tradition, we recognize that we live in a new media age, immersed in a new culture with an evolving language. We propose to make use of the most effective, most powerful means to communicate the integrations of faith and culture, which is at the center of Catholic values and education.

The Archdiocese of Detroit approved a plan to establish electronic connectivity between and among the Michigan Catholic Conference (MCC), diocesan offices, Sacred Heart Major Seminary (SHMS), The Edmund Cardinal Szoka Library, The Retreat Center at St. John's, parishes, schools, and social service agencies in and affiliated with the Archdiocese of Detroit through the use of local and wide area computer networks.

The Archbishop of Detroit is solicitous about unity, purpose, and consistency in the mission of the Church in its public image. Accordingly, the Archdiocese of Detroit offers these policies and procedures as a statement of principle to insure proper management and use of the equipment and services provided by the Archdiocese of Detroit and the internet connectivity provided by the MCC.

INTRODUCTION:

The policies and procedures presented herein apply to all users of the AODnet including but not limited to Central Service personnel, staff members, full-or part-time and temporary (volunteers), students, faculty, library patrons, and clients of the AODnet. These policies will address standards for utilization of electronic media and security.

The policies contained in the handbook supersede all other Computer Policy and Procedures. The Archbishop of Detroit reserves the right to amend or revise this document, in whole or part, at any time. The Archbishop of Detroit or the Moderator of the Curia will provide written notification of any change.

STANDARDS FOR UTILIZATION OF ELECTRONIC MEDIA:

1. BASIC POLICY

1.1. Clients of the AODnet increasingly use electronic forms of communication and information exchange. AODnet users may have access to one or more forms of electronic media and services (computers, e-mail, telephones, voice mail, fax machines, external electronic bulletin boards, wire services, on-line services, the Internet, etc.)

1.2. The Archdiocese of Detroit encourages the use of these media and associated services because they make communication more efficient and effective, and because they are valuable sources of information. The AOD recognizes that these communications and services can provide great benefits to individuals, the Church, and society as a whole. On the other hand, their inappropriate use can result in much harm. This policy is intended to deter clients from harmful use of these services, while allowing them the freedom necessary for productive, beneficial use.

1.3. Electronic media and services provided by the Archdiocese of Detroit are the said organization's property. Their purpose is to facilitate the business of the Archdiocese of Detroit and the business of its approved subsidiaries and partners.

1.4. With the rapidly changing nature of electronic and online services, this policy cannot lay down rules to cover every possible situation. Instead, it expresses the Archdiocese of Detroit's philosophy and sets forth general principles to be applied to use of electronic and online services.

1.5. The following procedures apply to all electronic and online services which are:

1.5.1. Accessed on or from AOD premises,

1.5.2. Accessed using AOD computer equipment, or via-AOD paid and/or supported access methods, and/or

1.5.3. Used in a manner, which identifies the individual with the AOD or its approved subsidiaries and partners.

2. PROCEDURES

2.1. Electronic media may not be used to knowingly submit, publish, or display any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive or otherwise illegal material; nor shall the user encourage the use, sale, or distribution of controlled substances. Any use in violation of any local, state or federal law is also prohibited and is a breach of the terms and conditions of this policy. Examples of forbidden transmissions include sexually explicit messages, cartoons, or jokes; unwelcome propositions or love letters; ethnic or racial slurs; or any other message that can be construed to be harassment or disparagement of others based on their sex, race, age, national origin, or religious or political beliefs.

2.2. Electronic and online services are primarily for business use. Limited, occasional or incidental use of electronic media (sending or receiving) for personal, non-business purposes are understandable and acceptable.

2.3. At no such time should AODNet services or property be used to conduct personal commercial business, using AODnet neither for private financial or commercial gains, commercial or private advertising, product advertisement nor for the establishment of personal Web pages.

2.4. Electronic information created and/or communicated by an employee using e-mail, word processing, spreadsheets, voice mail, telephones, Internet access, etc., will not generally be monitored by the AOD. The following conditions, however, should be noted:

2.4.1. All messages and related files are property of the AOD.

2.4.2. The AOD routinely monitors usage patterns for data communications (e.g. site accessed; peak utilization times; data volume). Reasons include cost analysis/allocation and the management of AOD communication equipment and services.

2.4.3. The AOD also reserves the right, in its discretion, to review any employee's or AODnet user's electronic files, messages, and usage to the extent necessary to ensure that electronic media and services are being used in compliance with the law and with this and other policies. There may also be other business or legal reasons to access or disclose any employee's electronic files or messages.

2.4.4. AODnet users should not assume electronic communications are totally private and confidential.

2.4.5. Since personal messages can be accessed by the AOD without prior notice, individuals should not use electronic communications to transmit any messages that should not be read by a third party. For example, individuals should not use AODNet e-mail for gossip, including personal information about oneself or others, for forwarding messages under circumstances likely to embarrass the sender, or for emotional responses to business correspondence or work situations. In any event, use of electronic media for such purposes as soliciting or proselytizing for commercial ventures, or personal causes or outside organizations or other similar, non-job related solicitations is prohibited.

2.4.6. The AOD, as well as the Michigan Catholic Conference (MCC), does monitor internet usage and sites accessed. This monitoring is routine and automatic. Individuals using internet services provided by the AOD can be linked to sites the individual visits and, through acceptance of this policy, agree to appropriate use as defined in this policy.

2.5. AODnet users must respect the confidentiality of other people's electronic communications and may not attempt to "hack" into other systems, or use other people's login IDs without

written authorization, or “crack” passwords, or breach computer or network security measures, or monitor electronic files or communications of other clients or third parties except by explicit direction per section 2.4.

2.6. Each employee who uses any additional security measures (e.g. password protected files, application specific passwords, etc.) on an AODnet connected computer or information service, must provide a sealed hard copy record (to be retained in a secure location) of all of his/her computer or information service passwords for AOD use if required to his/her immediate supervisor. (Example: there may be a need for the AOD to access an employee’s system or files when they are away from the office.)

2.7. No e-mail or other electronic communication may be sent which attempts to hide the identity of the sender, or represents the sender as someone else or from another company.

2.8. Electronic media and services should not be used in a manner that is likely to cause network congestion or significantly hamper the ability of other people to access and use the system. AODnet users must not deliberately or willfully use electronic media or services to cause damage to computer equipment or software, or assist others in doing so. (Example: deliberately spreading a computer virus.)

2.9. It is a violation of this policy for any employee, including system administrators and supervisors, to use outside applications (games, disks, personal software) on AOD office and laptop computers.

2.10. Anyone obtaining electronic access to other companies’ or individuals’ materials must respect all copyrights and may not copy, retrieve, modify or forward copyrighted materials except as permitted by the copyright law, copyright owner, academic use or a single copy for reference use only.

2.11. Any messages or information sent by an employee to one or more individuals via an electronic network (e.g., email, bulletin board, on-line service, Internet) are statements identifiable and attributable to the AOD. While some users include personal “disclaimers” in electronic messages, it should be noted that there would still be a connection with the AOD, and the statement might still be legally imputed to the AOD. All electronic communications sent by AODnet users must comply with this and other established policies, and may not disclose any confidential or proprietary information. AODnet users are responsible for protecting work product, including, but not limited to, data files and intellectual property.

2.12. “Chat” rooms can be an open communications forum for the exchange of many types of discussions. Topics could range from idle talk, to very personal and confidential concerns. Any advice or counseling provided through the use of a chat room, cannot provide the physical presence, and ability to assess the participants demeanor, thus creating liability for the counselor and for the AOD. In addition, the unmonitored nature of such a communications forum, could result in the posting of defamatory or offensive material. Therefore, the use of chat rooms is prohibited. An authorized alternative is the use of discussion groups.

2.13. Network services and Internet sites can and do monitor access and usage and can identify at least which company – and often which specific individual – is accessing their services. Thus accessing a particular website or online resource leaves identifiable electronic “tracks” even if the client merely reviews material. All internet activities must be in good taste, presenting a positive, professional image of both the employee or client and the AOD. AODNet users must practice appropriate “netiquette” customs. Use of inflammatory and offensive language (a.k.a. “flaming”) is prohibited.

2.14. An AODnet user’s access privileges to electronic media and services are determined by AOD management and not assumed.

2.15. Each employee’s use of electronic media and services must be appropriate to his/her tasks or job responsibilities.

2.16. All information created for broad public dissemination through electronic media must have prior approval by an immediate supervisor. This includes email messages to groups of people on and outside of the AODnet.

2.17. All email communication to more than one individual outside the AODNET should have the recipient’s addresses listed in the BCC field NOT the To... or Cc... field.

2.18. The AOD may create forms to facilitate the flow of information through electronic media. Modification of forms is prohibited without management approval.

2.19. Electronic games may be used during a regular scheduled break or during the lunch hour. AODnet users need to demonstrate, however, a sense of responsibility and may not abuse the privilege. Games or other entertainment activities that communicate using the AODnet or the Internet are prohibited.

2.20. Access to the AOD system through home and/or private computers is allowed only after agreement by the immediate supervisor and the AOD Office of Information Technology. Access of this nature is by default not allowed.

2.21. Any employee or client found to be abusing electronic media or services will be subject to corrective action up to and including the termination of services and/or employment.

SECURITY:

3. BASIC POLICY

3.1. The Archdiocese of Detroit Office of Information Technology will be responsible for security of AODnet.

3.2. All Fax cover sheets will contain the following statement:

The information contained in this communication is privileged and confidential and is intended solely for the use of the individual(s) to whom this communication is directed. If the reader of this communication is not the intended recipient, you are hereby notified that any dissemination, distribution, or copying of this communication is strictly prohibited. If you have received this communication in error, please notify us immediately by telephone and return this communication to us via the United States Postal Service. Thank you.

4. PROCEDURES

4.1. Security of Archdiocese of Detroit communications and data, is the cornerstone of the AODnet. These security policies and procedures extend to each unit becoming a part of the Archdiocese of Detroit system. AODnet information is considered confidential, and must be protected from public access. Unit members must ensure that adequate security measures have been taken to protect data. These measures include but are not limited to, power on passwords, network or operating system passwords (if applicable), data encryption, and limiting access to equipment by authorized personnel only.

4.2. Use of a public Internet Service Provider outside that of the Archdiocese of Detroit system, can, in certain circumstances, present a security risk. Because of the diversity in connection styles and ingenuity of some individuals in our current day society, use of a public Internet Service Provider in addition to that of the AODnet, is prohibited.

(Example: Using a modem, including cable, to connect to an ISP when that PC is connected to the AODnet.)



UTILIZATION OF ELECTRONIC MEDIA

USER AGREEMENT FORM

- I have read and understand the “Computer Policies and Procedures for the Archdiocese of Detroit”
- I understand that access to AODnet, Internet, e-mail and other forms of electronic access is for the benefit of the Archdiocese of Detroit and its approved subsidiaries and partners.
- I agree to abide by the policy as stated in the “Computer Policies and Procedures for the Archdiocese of Detroit”. I further understand that should I commit any violation, my privileges may be revoked and disciplinary and/or appropriate legal action may be taken.
- In consideration for using AODnet and having access to public networks, I hereby release the Archdiocese of Detroit and its Board members, employees, and agents from any claims and damages arising from use, or inability to use the services being provided.
- I understand the use of the AODnet and its services is designed for the business and educational purposes and that the Archdiocese of Detroit cannot eliminate all controversial material. I recognize it is impossible for the Archdiocese of Detroit to restrict access to all controversial and inappropriate materials. I will hold harmless the Archdiocese of Detroit, its employees, agents, or Board members, for any harm caused by information or services provided by or obtained via the network.

Signature

Date

Name (print)

Title