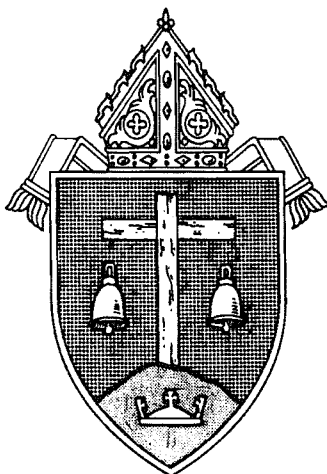


DIOCESE OF MONTEREY



**Diocesan Policy Regarding Access
To and the Use of Diocesan Data and
Computer Hardware/Software and
the Use of the Internet and E-mail
by Diocesan Employees, Clergy,
Religious and Seminarians**

Diocesan Policy
Regarding Access To and the Use of
Diocesan Data and Computer Hardware/Software
and the Use of the Internet and E-mail
By Diocesan Employees, Clergy,
Religious and Seminarians

1. Introduction

- 1.1. Information technology is increasingly becoming an integral part of the day to day operations of the Diocese of Monterey. The Diocese must take appropriate steps to ensure that information technology is properly protected and utilized. Towards that end, it is the responsibility of diocesan personnel to protect these resources.
- 1.2. The Diocese of Monterey furnishes its employees, and other authorized users, hereafter jointly known as “users”, with access to information technology, including personal computers, local area networks, remote access capabilities, computer applications, etc., for the purpose of enabling them to fulfill their job responsibilities. This information technology, data and records are the property of the Diocese and are to be used for Diocese of Monterey business purposes only.

2. Security of Diocesan Data

- 2.1. All data utilized on diocesan computer equipment is the property of the Diocese of Monterey. The Diocese will maintain a system of information security to protect its proprietary data. Integral parts of this system are the policies, standards, and procedures designed for use by users. All users must adhere to these policies, standards, and procedures for the complete system to remain viable. These policies, standards, and procedures include, but are not limited to maintaining data confidentiality; maintaining the confidentiality of data security controls and passwords; and immediately reporting any suspected or actual security violations or breaches.
- 2.2. The Diocese of Monterey prohibits the use or alteration of diocesan data and/or information technology without proper authorization.

- 2.3. All users continue to have an obligation to protect the confidentiality and nondisclosure of proprietary, confidential and privileged data as well as personally identifiable information whether communications occur through diocesan computer systems or otherwise. If in doubt about whether an electronic transmission would violate an obligation of confidentiality or nondisclosure, a user should seek advice from his or her supervisor, department director and/or diocesan legal counsel identified by the Chancellor.

3. Use of Electronic Mail & Internet Use

- 3.1. The Diocese provides and maintains an electronic mail ("e-mail") system for the purposes of communicating through written, electronically transmitted form with each other and others outside the Diocese. E-mail is specifically for users and intended for authorized business purposes only. Special attention should be paid to communication directed to individuals outside of the diocesan system such as Internet e-mail recipients and the receipt of information from Internet mail.
- 3.2. The connection of diocesan systems to the Internet exists so that communication can take place among diocesan staff and with the public outside of the diocesan local area network. This service is to be used strictly for business purposes.
- 3.3. Users should not have an expectation of privacy regarding e-mail and internet use. All e-mail and internet use is subject to review by respective department directors and supervisors.
- 3.4. In an effort to preserve the integrity of security systems in place on the diocesan local area network, any or all user connections to the Internet may be interrupted by the Computer Services Manager at any time and without warning if conditions warrant.
- 3.5. Any software or files downloaded off the internet become the property of the Diocese of Monterey. All downloaded files should be scanned for viruses before use.
- 3.6. Users are not permitted to access the Internet or e-mail services via the services provided by Diocese of Monterey information systems without permission from their supervisor or department director. Internet or on-line access shall be limited to business purposes only. Users who inappropriately use the e-mail and/or internet access may be subject to disciplinary action up to and including dismissal.

4. Diocesan Network/User Accounts

- 4.1. The ability of an individual to access the diocesan network, e-mail system, and all data contained therein will be controlled by means of a user account. A user account consists of a unique user name, confidential password (by user or department), and all information describing what resources the specific user can access, at what level, and during what time periods. All passwords are confidential and should not be shared. Passwords will not be administratively revealed to any person, with the exception being the Computer Services Manager, Department Director and Chancellor. Passwords will be changed only when authorized by the user's supervisor or Computer Services Manager. All passwords must be given to the Computers Services Manager, who in turn will provide them to the Chancellor.

5. Unauthorized Use / Content of Communications

- 5.1. The Diocese strictly prohibits any transmission of electronic communications that would be conduct or communications contrary to diocesan policy. Engaging in conduct or communications prohibited by diocesan policy may lead to discipline up to and including dismissal.
- 5.2. Examples of prohibited communications include, but are not limited to:
 - 5.2.1. Communications, materials, information, data or images that are obscene, pornographic, sexually explicit or offensive, threatening, abusive, harassing, discriminatory, or in violation of any diocesan policy or contrary to the mission or values of the Diocese, including disparagement of others based on race, national origin, marital status, gender, age, disability, pregnancy, religious or political beliefs or any other condition or status protected by federal, state, or local law.
 - 5.2.2. Communications, materials, information, data or images that may constitute verbal abuse, defamation (libel or slander), fraud or misrepresentation, or trade disparagement of users, employees, customers, clients, competitors, vendors or any other person or entity.
 - 5.2.3. Accessing, viewing, printing, storing, transmitting, disseminating or selling any information protected by law or subject to privilege or an expectation of privacy.
 - 5.2.4. Accessing, creating, distributing, engaging in or soliciting sexually oriented messages or images, unwelcome sexual advances, requests for sexual favors or other unwelcome conduct of sexual nature.
 - 5.2.5. Any attempts to access, monitor or disrupt information that is restricted, confidential or privileged and to which the user has not expressly been authorized access.
 - 5.2.6. The intentional or diligent introduction of a computer virus into the system or causing damage to data or the system.
 - 5.2.7. Granting access to unauthorized persons, either by intentional action such as disclosure of account information or unintentional action such as failure to log off.
 - 5.2.8. Unauthorized removal, deletion or duplication of data, software or hardware.
 - 5.2.9. Violations of software license agreements.
 - 5.2.10. Development or use of unapproved mailing lists.
 - 5.2.11. Use of technology system for private business purposes unrelated to the business of the Diocese.
- 5.3. Personal use of diocesan information technology is not permitted except as authorized by a user's supervisor or the Chancellor.

6. Personal Computer Software Policy

- 6.1. Federal Copyright Act protects most computer software. In accordance with copyright laws, diocesan users are prohibited from making illegal copies of computer software or from installing software from illegal copies. Users are prohibited from installing software brought in from home, as this is a copyright violation. Conversely, installing software intended for use on a diocesan system on a home computer is a violation of copyright and is expressly prohibited
- 6.2. All software to be used on diocesan computer systems is to be installed by the Computer Services Manager. Users are prohibited from installing or running software on diocesan systems without prior approval of the Computer Services Manager.
- 6.3. Except as otherwise expressly authorized, the Computer Services Manager will centrally acquire and install all software to be used on diocesan systems.

7. Right of Inspection

- 7.1. The Diocese of Monterey reserves the right to inspect and examine any Diocesan owned or operated communications system, computing resource and/or files or information, including diocesan personal computers, area networks, applications, and e-mail, contained therein at any time. These systems may be subject to periodic unannounced inspections and should be treated like other shared filing systems. Users have no privacy right to any data, information or documents received or disseminated on the network, internet or through e-mail. The content of e-mail messages and computer files, properly obtained for legitimate business purposes may be disclosed within the Diocese without employee permission. Therefore, you should not assume that messages and files are confidential. By utilizing these diocesan systems, users consent to the Diocese's right to inspect and examine all data, information, documents and e-mail.
- 7.2. When a user acts inappropriately through the technology system, the Diocese may report such actions to any outside authorities and/or take appropriate internal Diocesan disciplinary action.
- 7.3. When sources outside the Diocese request an inspection and/or examination of any diocesan owned or operated technology system, computing resource and/or files or information contained therein, the Diocese will treat the information as confidential unless any one or more of the following conditions exist:
 - When approved by the appropriate Diocesan official(s) to whom the request is directed;
 - When required by federal, state or local law; or
 - When required by a valid subpoena or court order.

8. Compliance

- 8.1. The above policies apply to diocesan information technology and all users of diocesan information technology. Use of these resources indicates acceptance of these policies.
- 8.2. Violations of the terms and conditions of the Policy may subject users to loss of technology access, as well as other disciplinary action up to dismissal. Illegal acts involving diocesan computing resources may also subject violators to prosecution by local, state and/or federal authorities.

ACKNOWLEDGMENT AND ACCEPTANCE OF DIOCESE OF MONTEREY INTERNET AND E-MAIL APPROPRIATE USE POLICY

As an employee of the Diocese of Monterey or as an authorized user of diocesan information technology, I have received and read the Diocesan Policy Regarding Access To and the Use of Diocesan Data and Computer Hardware/Software and the Use of The Internet and E-mail By Diocesan Employees. I understand and agree to abide by the policies and guidelines described herein and have had the opportunity to ask questions about the policy.

I further understand that I do not have a right to privacy in any diocesan provided technology and that any violation of this policy may result in disciplinary action. Such action may include suspension or revocation of internet privileges, suspension or dismissal from employment and/or legal action.

I understand that users are subject to all local, state, and federal laws and that illegal activities may be reported to the appropriate law enforcement authorities. I agree to report any violation of this policy I observe to my department director or to the Diocese of Monterey Human Resources Director.

No one, except the Bishop, has authority to make any oral or written representations inconsistent with the policies, practices and regulations contained in these policies. The statements in this document supercedes all written and oral representations that are in any way inconsistent with them.

Name

Signature

Date