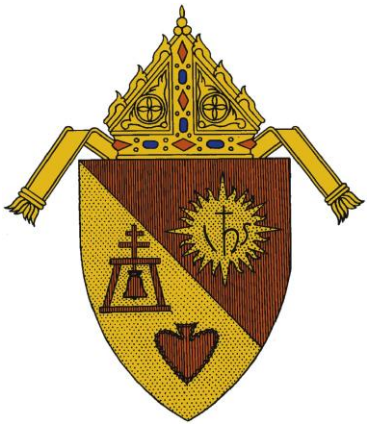


DIOCESE OF SAN BERNARDINO

DIOCESAN ELECTRONIC COMMUNICATION POLICY

APRIL 1ST, 2011

1201 E. Highland Ave., San Bernardino, California 92404-4641
Phone: (909) 475-5400 Fax: (909) 475-5155 Support: (909) 475-5409
Email: informationservices@sbdiocese.org

ELECTRONIC EQUIPMENT USAGE

POLICIES AND PROCEDURES

STATEMENT OF PURPOSE:

The purpose of this policy is to assure protection of Diocesan computer system security and assets, to protect the privacy rights of employees, to manage Diocesan resources, and to protect the rights of third parties for appropriate access to Diocesan files.

The efficiency and creativity that our computer systems provide to us have also brought forth many legal and moral obligations that we must seriously consider. The policy and procedures set forth in this document are intended to address several areas so that we are able to protect user privacy rights, system security requirements and proper stewardship of Diocesan resources and assets.

This document is divided into two main sections; section (1) addresses your rights and obligations relevant to Diocesan owned equipment, section (2) addresses the technical aspects and usage requirements of Diocesan owned equipment. We believe that by providing clear guidelines and specific usage policies we can prevent confusion as well as enable users to properly utilize electronic equipment in the performance of their ministry duties.

POLICY:

This document sets forth Diocesan policy with regard to access and use of computer hardware, software, data, and electronic mail messages. It also sets forth the Diocesan policy with regard to disclosure of computer files, created or received, or electronic mail messages sent or received by Diocesan employees with the use of the Diocese's computer resources or electronic mail system.

This document sets forth policies on the proper use of computer hardware, software, data, and the electronic mail system provided by the Diocese of San Bernardino.

The Diocese of San Bernardino intends to honor these policies but reserves the right to change them at any time it may deem reasonable under the circumstances.

All employees that utilize Diocesan computers are responsible for reading and adhering to these policies. It is the responsibility of supervisors to ensure that each of their employees has received this document and signed off that they have read it, understand it and agree to abide by it as a condition of employment.

INTRODUCTION:

Information and technology are increasingly becoming an integral part of the day-to-day operations of the Diocese of San Bernardino. It is the responsibility of Diocesan (parish, pastoral center, schools, Diocesan entities etc.) personnel to protect these resources. The Diocese of San Bernardino must take appropriate steps to ensure that information and technology are properly protected and utilized.

The Diocese of San Bernardino furnishes its employees, volunteers, and other authorized users, hereafter jointly known as "users", with access to information technology. This includes computer systems (workstations, laptops, tablets, etc.), local area networks, remote access capabilities, computer applications, etc., for the purpose of enabling them to fulfill their job ministry responsibilities. This information technology, data, and records are the property of the Diocese of San Bernardino and are to be used for the Diocese of San Bernardino business purposes only.

The Diocese of San Bernardino reserves the right to inspect and examine any Diocesan owned or operated communications system, computing resource and/or files or information, including computers systems, local and WAN area networks, applications, and e-mail, contained therein at any time. Therefore, users shall have no expectation of privacy with regards to any data, information or documents received or disseminated on the network or through e-mail. By utilizing these Diocesan systems, users consent to the Diocese's right to inspect and examine all data, information, documents, and e-mail.

Privacy

The Employee should not expect that any communication made via any electronic communication is private. As a matter of routine, the Diocese will not monitor e-mail, voice mail messages, or facsimiles. However, should it become necessary, all procedures will be conducted in accordance with federal and state laws. In regards to the usage of equipment located in the Diocese at the Pastoral Center and used by employees anywhere within the Diocese, the Diocese, through its Directors and the Director of Information Services, reserves the right to review the contents of employees' e-mail, voice-mail files or facsimiles at its sole discretion. Also, employees may not intentionally intercept, eavesdrop, record, alter or receive other persons' e-mail or voice mail messages or facsimiles without proper authorization.

ELECTRONIC COMMUNICATION

Proper Use

The data storage, e-mail, voice mail, and facsimile systems are Diocesan property and are intended for Diocesan business. The systems are not to be used for employee personal gain, or illegal activities. All data and other electronic messages within these systems are the property of the Diocese of San Bernardino, but the employee should not expect that any communications made are confidential or private. The Diocese, in its sole discretion, reserves the right to access, review and save any communication, whether "personal" or work-related. See Section IX. Permission for limited and brief personal use of e-mail, voice mail, and facsimile must be obtained by the staff person's office director.

Prohibited communications

Examples of prohibited communications include, but are not limited to:

1. Communications, material, information, data or images prohibited by legal authority as 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, sex, age, disability, pregnancy, religious or political beliefs or any other condition or status protected by federal, state or local laws.

2. Communications, materials, information, data or images that may constitute verbal abuse, libel or slander, defamation, fraud or misrepresentation or trade disparagement of users, customers, clients, competitors, vendors or any other person or entity.

3. Accessing, viewing, printing, storing, transmitting, disseminating or selling any information protected by law or subject to privilege or an expectation of privacy.

4. Accessing, creating, distributing or soliciting sexually oriented messages or images, unwelcome sexual advances, requests for sexual favors or other unwelcome conduct of sexual nature, including jokes.

5. Any attempts to access, monitor, or disrupt information that is restricted, confidential or privileged and to which the individual has not expressly been authorized access.

6. The intentional or diligent introduction of a computer virus into the system or causing damage to data or the system.

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 computer system or lock computer system.

8. Unauthorized removal, deletion or duplication of data, software or hardware upon a user's termination or departure from the Diocese.

9. Violations of software license agreements.

10. Development or use of unapproved mailing lists.

11. Use of technology systems for private business purposes unrelated to the business of the Diocese of San Bernardino.

12. Academic dishonesty.

13. Disclosure of personal or private information about an employee or minister of the church without their prior written consent.

Sensitive Issues

The e-mail, voice mail and facsimile systems should not be used to transmit sensitive material such as personnel decisions, reprimands or material that is confidential in nature. Avoid language that is insensitive, insulting, offensive, derogatory, harassing, or discriminatory. If you are in doubt whether electronic communication is the proper medium for a message, use another form of communication.

Section One

GENERAL

Work Product Ownership

All information developed on a Diocesan computer system or introduced to a Diocesan computer system is the property of the Diocese of San Bernardino, regardless of where it was created.

Likewise, all information developed by a Diocesan employee on computers outside of the Diocese of San Bernardino, if in conjunction with his or her employment with the Diocese of San Bernardino is the property of the Diocese of San Bernardino. Copies of such files must be provided to the Diocese, which has exclusive rights to retain, maintain, and modify these files.

In some circumstances, written permission for the use of material developed as stated above may be obtained. Requests for permission should be made to the users' supervisor through the employees' office director.

PERSONAL USE OF DIOCESAN SYSTEMS

Brief use of information systems (computers, etc.) for personal purposes is allowable only when the use meets the following criteria:

1. The staff members' supervisor gives authorization. This must be obtained prior to any first usage.

2. Serves a legitimate public interest, serves to educate Diocesan staff on the use of Information Systems, serves to improve the morale of Diocesan staff or serves to enhance the professional skills of the employee.

3. Does not put Diocesan Information Systems to use that would reflect adversely upon the Diocese of San Bernardino.

4. Does not overburden the communications system (such as may be the case with broadcast and group mailings, video transmissions, audio playback) and does not create any significant additional cost to the Diocese.

In addition, personal communications from the work place that are most reasonably made while at the work place (such as checking in with a spouse or minor children; scheduling doctor and auto or home

repair appointments or emailing directions to visiting relatives) are examples of acceptable uses with the understanding that excessive personal activity is subject to discipline pursuant to Diocesan personnel policies.

Other organizations will not use the Diocese of San Bernardino computers. Due to the complex configuration of the Diocesan network and support issues, this would not be practically possible.

ELECTRONIC MAIL AND OTHER PRIVACY ISSUES

The Diocese of San Bernardino provides for all employees and maintains an electronic mail ("e-mail") system for the purpose of communicating through written, electronically transmitted form with each other and others outside the Diocese of San Bernardino. E-mail is specifically for users and intended for authorized business purposes only. Basic guidelines for using electronic mail (E-mail) or any other form of data as a Diocesan employee:

- ✓ Tact counts. If there is any doubt whether e-mail is the right medium for a message, use another form of communication.
- ✓ If you are a supervisor, never deliver a reprimand via e-mail.
- ✓ Never gossip or provide personal information about yourself or someone else or emotional responses via email.
- ✓ The use of insensitive language or derogatory, offensive, threatening or insulting remarks is subject to discipline per Diocesan Human Resource policies and practices.
- ✓ The use of harassing language of any type, including sexually harassing language or any remarks that may be misinterpreted as such is subject to discipline per Diocesan Human Resource policies and practices.
- ✓ E-mail is not confidential and will be periodically reviewed.

In other words, use common sense and our gospel values, keeping in mind the Diocesan vision statement.

Section Two

GENERAL

Storage of Data

1. Networked Computers: All data shall be stored on network servers in defined storage areas.

2. Non-networked Computers: All data is stored on the local hard drive and should be stored in well-defined folders. If systems become networked in the future, data is to be transferred to the network server. Data should not be stored on USB flash devices except for backup procedures, and transporting to another computer system. See section on portable files below.

3. Pastoral Center: All data shall be stored on network servers. The Office of Information Service does not back up the local workstation hard drive (the C: drive). Also, the process of re-configuring workstations as the environment changes may at any time result in the loss of data stored on the workstations hard drive.

4. Schools and Parishes: All data should be stored on network servers if they are available. If a location does not have a networked storage device (server or other type), then that location should consider implementing one and consult with the Director of Information Services of the Diocese.

Backup procedures

Computer software data files are to be backed up on a regular schedule. In general, this consists of full weekly backups of all data, and differential daily backups of data to appropriate media (tape, CD-ROM, hard drives, off-site storage). Typically, detailed backup procedures are documented for the software programs you are using. The Information Services office has detailed backup procedures documented primarily for the ParishSOFT line of software programs and for our general file storage system. These procedures can be applied to any and all computer systems and networks.

Software applications must be closed (exited) at night so that no "open files" exist. Open files cannot currently be backed up.

Management of Files

Users of computer systems are expected to manage their computer-generated files. Files should be saved in appropriately named folders to assist in retrieval of those files. Outdated files should be deleted. Permanent files are those files that are used on a regular basis. Following proper backup

procedures, deleted files can be recovered if needed in the future. Whether on a stand-alone workstation or a network, consideration must be given with regards to storage space. Personal files (pictures, videos, audio, etc.) should never be stored in networked storage areas.

Pastoral Center: Because the storage capacity of the network is limited, all users are responsible for deleting outdated files. Files that are older than three years on the office directory and older than two years in employees' personal directories are considered outdated. It is acknowledge that some files are to be retained for many years. The Office of Information Services will periodically, delete any files that are outdated. Users will be notified of this action in advance. Personal files will also be deleted as those files should never be stored on Diocesan networked storage devices.

Portable Files

To facilitate off-site work, employees may copy appropriate files to and from external storage devices, such as USB flash drives. Appropriate files include word processing documents, electronic spreadsheets, videos and presentation graphic files (examples include files created in MS Office Word, Excel, or PowerPoint). Any external storage devices used in computers outside of the Diocese of San Bernardino must be checked for viruses prior to being used in a Diocesan computer. No other files or information may be copied from or to Diocesan computers.

Licensed Software

The Diocese of San Bernardino complies with all software copyrights and terms of all software licenses. Diocesan employees may not duplicate licensed software or related documentation. Any such duplication may subject employees and/or the Diocese to both civil and criminal penalties under the United States Copyright Act. Employees who engage in such activity are also subject to discipline pursuant to Diocesan personnel policies. Diocesan-owned software may not be loaded on to external systems unless the license agreement allows such use and the Director of Information Services approves. Also see section, **SOFTWARE USE AND THE LAW.**

Configuration

Computer systems and equipment are configured to operate in a complex, networked environment. **Users may not change their system's setup files.** Users who believe their setup files are not configured correctly should contact the primary person assigned to manage the computers for assistance.

At the Pastoral Center, this would be Information Services.

Acceptable Use

The purpose of using information systems within the Diocese of San Bernardino is to enhance the ability of individuals to conduct Diocesan business and ministry, except as outlined in section Personal Use of Diocesan Systems. The use of computer systems must be in support of the general mission of the Diocese of San Bernardino and consistent with its objectives.

At the end of the workday, users should at a minimum turn off their computer monitors and printers. Computer systems are optional, but during summer hours it may be requested of users to turn off their computer systems due to the potential of electrical blackouts.

Pastoral Center: At the end of the workday, users must close all applications and turn off their monitor and printer (the computer should be left on). Before leaving work on Fridays, users should restart their computer systems and leave the computer at the user log-on screen.

SECURITY

Overview

Electronic information is a significant asset of the Diocese of San Bernardino. 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 our 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, attempted, or actual security violations or breach.

Virus Protection

Computer viruses pose a serious threat to the integrity of both the computer technology and data assets of the Diocese. Computer viruses are designed to be destructive to both computer systems and data. In a networked environment such as exists in the pastoral center, the inadvertent introduction of a virus to one desktop computer system could result in the infection of every system connected to the network in a matter of moments. Users shall not change their systems configuration or take other steps to defeat virus protection devices or systems.

Individual employees are responsible for verifying that storage devices used or received from outside computers are scanned for viruses prior to their use in Diocesan computers. All workstations and

servers should be updated with the latest anti-virus protection program and data files. Contact the Office of Information Services for assistance in having the diskettes checked. The current standard anti-virus program is "Virus Scan" from McAfee or Norton Anti-Virus from Symantec.

Control of Security

Users shall not add additional security, such as passwords, to their workstations or files. Encryption methods should only be used for the transfer of files between two locations. Files should be returned to an unencrypted state following such transmission. Users who believe they have security needs that go beyond current information technology standards and tools should contact the primary person responsible for the computer systems.

At the Pastoral Center, contact the Office of Information Services.

Access to Data

The users' ability to view, add or modify information in network files is based on access rights configured on the network. These configurations can be changed as needed. The Diocese of San Bernardino prohibits the use or alteration of Diocesan data and/or technology without proper authorization. Contact the primary person responsible for the computer system to request changes to user access rights.

At the Pastoral Center, contact the Office of Information Services.

User Access Controls

Computer users shall identify themselves to the system by signing on with their assigned user name. Users shall never attempt to sign on to the system with any other user name. 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 computers systems or otherwise. If in doubt about whether an electronic transmission would violate an obligation of confidentiality or nondisclosure, a user must seek advice from his or her supervisor, department head, and/or legal counsel identified by the Chancery.

Password

Passwords are confidential informational items that should never be shared with other individuals. This is to protect the security of the computer systems and files. If you feel that your password has been compromised, you should request to have your password changed immediately. It is the responsibility of the individual to remember his or her password. Passwords should never be written on anything or stored in proximity to a user's computer system.

Faxes

All Fax cover sheets will contain the following statement:

The information contained in this facsimile message is legally privileged and confidential information, intended only for the use of the individual(s) or entity to which 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 at the above address via the United States Postal Service. Thank You.

Vandalism

Vandalism cannot be tolerated. Vandalism is defined as any malicious attempt to harm or destroy data of another user, network, or agency that is connected to the Internet. This includes, but is not limited to, the purposeful uploading or downloading of any computer viruses, attempts at gaining unauthorized access to information, or changing on-line material without permission.

SOFTWARE USE AND THE LAW

In addition to authorized roles regarding software, the legal implications for improper handling of software can be significant:

According to the U.S. Copyright Law, illegal reproduction of software can be subject to civil damages of as much as $100,000 per work copied, plus criminal penalties, including fines and imprisonment. The Diocese of San Bernardino does not condone the illegal duplication of software or any other form of criminal activity. Employees who engage in such activity are also subject to discipline pursuant to Diocesan personnel policies.

All software to be used on Diocesan computer systems is to be installed by the primary person responsible for the computer systems. Users are prohibited from installing software brought in from home, as this is often 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 unless authorized in the licensing agreement with the software manufacturer.

Call the Director of Information Services at 909-475-5400 if you would like more information on software use and the law.

At the Pastoral Center, a member of the Information Services office will install the software. Users are prohibited from installing or running software on Diocesan systems without approval of the proper designated individual within the Office of Information Services

PORTABLE COMPUTER USAGE (PASTORAL CENTER)

Portable computers (e.g. laptops, PDA's, tablets, etc.) are available for Diocesan business outside of Diocesan facilities, and after normal working hours provided these procedures are followed:

- ✓ If a portable computer is stolen while outside of Diocesan facilities, an insurance claim should first be submitted to the individual's insurance company. A police report will be required and should be obtained immediately.
- ✓ If the individual's insurance company pays for the theft, the check should be signed over to the Diocese of San Bernardino and given to the Accounting office.
- ✓ If the insurance company does not pay, the letter of denial should be forwarded to the Office of Risk Management. A copy of the police report should also be forwarded.
- ✓ There are several laptops available through the Media Center.
- ✓ Portable computers will be checked out on "first come, first serve" basis. The Media Center can assist you with this.

An employee may use Diocesan portable computers only for Diocesan work and in conformance with the Personal Use Policy section.

ELECTRONIC COMMUNICATION

Electronic communications can take a variety of forms such as telephone messages, voice mail, facsimile, electronic mail, and similar computer-based documents.

Electronic communication is any message or data sent or received electronically. There are three main categories of electronic communication currently being utilized by the Diocese: Electronic mail, voice mail, and facsimile. Electronic mail or e-mail is computer based and involves receiving and delivering some type of computer output (messages, letters, memos, spreadsheets, etc) via the Diocesan network and phone lines. Voice mail is a system whereby sounds, usually voices, are digitally recorded, transmitted, and stored. Facsimile communication is done via fax machines whereby information on paper is transmitted from one location to another, or to many locations. The Diocese of San Bernardino's e-mail, voice mail, and facsimile systems are provided to facilitate Diocesan business

communication among employees and other business associates. To assure the continued benefits that e-mail, voice mail, and facsimile makes possible it is necessary for all employees using these forms of communication to adhere to uniform policies.

Day Long Absence (pastoral center)

For absences of one day or longer, the Out of the Office Assistant (O.O.A.) in Microsoft Outlook should be used for the e-mail system. The O.O.A. is found under the "Tools" menu when using the "inbox". The temporary voice mail greeting should also be activated for the voice mail system. When leaving a message in the O.O.A. or in the temporary voice mail greeting, please remember to state what day or days you will be gone and leave the name of someone who can be contacted in your absence. Remember to make arrangements with your alternate contact on days when you will be gone.

Checking E-mail and Voice mail:

Both e-mail and voice mail should be checked at least daily. If the message requests a response the response should be sent as soon as possible. Receipt of an external message should be acknowledged immediately even if a subsequent response is required.

Voice Mail Greeting Messages

Voice mail greetings should be modeled after the examples supplied to the employees. Every greeting must give the caller the option to talk to a real person (by pressing zero).

Please be aware that all electronic communications reflect on the Diocese of San Bernardino and should be business oriented and professional in content. In other words, use common sense and focus on Diocesan business.

Deleting Messages

Generally, e-mail and voice mail messages are temporary communications, which are non-vital and may be discarded routinely. However, depending on the content of the message, it may be considered a more formal record and should be retained pursuant to a departments record retention schedule.

E-mail Address

To facilitate use of the e-mail system, you may give your individual e-mail address to professional associates, vendors and other business contacts. An individual's e-mail address at the pastoral center is configured as: first name initial (no space) last name @sbdiocese.org. For example: Jane Doe would be jdoe@sbdiocese.org. Additional e-mail addresses can be created if necessary.

- ✓ The Office of Information Services will administer a deletion of e-mail messages as needed to maintain storage capacity on Diocesan network servers. Users will be notified of deletions prior to the actual deletions taking place. Typically, users should keep only 6 months of deleted and sent items in their Outlook mailbox. Items in their Inbox should be kept for a short period of time, but if needed to be stored longer then items should be moved into folders in their Inbox area.

E-mail should be checked at least daily unless the individual is away from the office. When away from the office, e-mail can be checked via the Internet at the following site: **https://mail.sbdiocese.org/exchange/**

Direct Inward Dial (DID) (pastoral center)

It will be at the discretion of the employee to give his or her Direct Inward Dial (DID) or other phone number to others.

Junk mail (Spam)

Delete junk mail as soon as possible. Do not reply with an e-mail that asks to be deleted from any e-mail list unless you know the sender. Unsolicited spam emails confirm your email address if you respond to them and this causes you to receive even more spam messages. In Outlook, you can also add the senders' e-mail address to the "junk e-mail sender" list.

Graphics

Graphics require a lot of memory. ***Please limit distribution of graphics.*** If you receive messages with a graphic please delete it as soon as possible. Animations require large amounts of hard drive space and memory and should be avoided. If you receive animated emails, they should be deleted as soon as possible. Graphically created email should not be sent. Email should be kept plain and simply. The Diocese has office users outside the pastoral center that download email at slower speeds and graphical emails can take a long period of time to download. This places a burden on those users and cost money in time and phone charges.

Calendar/Scheduler Use Policy

All employees who have the Microsoft Outlook program are encouraged to use the calendar/scheduler program to facilitate the scheduling of all appointments and meetings.

All meetings, vacations and appointments should be updated daily on calendars.

Use the "set up meeting" function to schedule meetings with other staff members or groups.

When scheduling a meeting, be sure the reminder option is turned on. Set the reminder to come on prior to the meeting time. Staff members will get a reminder for the meeting and will not be late.

Travel time should be included when scheduling time yourself or through the Meeting Planner. When you create the meeting, you can note the meeting time and travel time in the comment section. You can also list the travel time as a separate time slot.

INTERNET USE

The use of the Internet during work hours should be limited to those subjects that are directly related to an individual's job duties for the Diocese of San Bernardino. Employees are advised to exercise discretion when using the Internet for work-related business since individuals outside the organization can monitor any Internet usage. The Office of Information Services and Human Resources will monitor computers connected to the Pastoral Center and our schools.

The primary function of the computer system is to assist in service delivery to our employees. Allowing employees to spend work time learning how to use and conduct research on the Internet will ultimately result in improved performance as employees for Diocese of San Bernardino.

To that end, employees may access web sites for work-related use after business hours. This use is limited to web sites that are considered business appropriate and employees are expected to exercise good judgment when accessing sites. Employees may not intentionally access any site that is inappropriate for the Diocese of San Bernardino, or which could cause embarrassment to the organization or the employee. If this occurs, employees are expected to notify their Supervisor. The Diocese of San Bernardino is held to a high standard of scrutiny and ethical behavior. Some examples of inappropriate sites include adult entertainment, sexually explicit material, web sites promoting violence or terrorism, illegal use of controlled substances (drugs) and intolerance of other people/races/religions, etc.

Files downloaded from the Internet should only be work-related. If such files need to be taken off premise for any reason, the preferred method is to electronically e-mail the file(s) to the other location

if possible. If that is not possible, files can be transferred to external storage devices. After being transported to another location, files should be deleted from the external storage device. Employees who engage in inappropriate or excessive non-work-related use of Internet are subject to discipline pursuant to Diocesan personnel policies.

RIGHT OF INSPECTION

The Diocese of San Bernardino reserves the right to inspect and examine any Diocesan owned or operated communications system, computing resource and/or files or information, including personal computers, local and WAN area networks, applications, and e-mail, contained therein at any time. Users have no privacy right to any data, information or documents received or disseminated on the network or through e-mail. By utilizing these Diocesan systems, users consent to the Diocese's right to inspect and examine all data, information, documents, and e-mail.

When a user acts inappropriately through the technology system, the Diocese reserves the right to report such actions to any outside authorities and/or take appropriate internal Diocesan disciplinary action.

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; or
- When required by federal, state or local law; or
- When required by a valid subpoena or court order.

Note: When law, court order, or subpoena requires notice, users will receive prior notice of such disclosures (viewing information in the course of normal system maintenance does not constitute disclosure).

Pastoral Center: Office directors shall make requests for inspection to the Director of Information Services. The department head for the Ministry of Communication shall then approve this request. Consultation shall also occur with the Chancellor of the Diocese.

DEFINITIONS

Diocese: In this document, the term Diocese will refer to the Diocese of San Bernardino.

Computer Storage Media: This refers to computer hard disks, tapes, compact disks (CDs), USB flash memory devices, or any other media used to store data used on portable computers or microcomputers.

Technology Committee: A review and approval committee comprised of Diocesan staff, parish members, and community members.

Electronic Mail (E-Mail): A network application that allows the network users to exchange electronic messages with one another. E-mail can allow users to attach computer files to the message, print a message, and send the same message to many users at once.

File Server: A computer that provides network stations with controlled access to shareable resources.

Local: Any device that is physically present at your workstation. The term refers most often to hard disk and USB flash memory devices.

Local-Area-Network (LAN): Describes a method of linking, generally by cables, personal computers in a specific work area, such as, a department or an office. Networked PCs can share data and resources such as file storage space, software, and printers.

Microcomputer (Micro): Computers that use miniature chips or microprocessors. Microcomputers are also called personal computers, PCs, or workstations.

Multi-user Access: More than one computer user can access an application or database concurrently.

Network Administrators: In this document, the term Network Administrators refers to the Director of Information Services.

Network Server: See File Server

Personal Computer (PC): See Microcomputer and Workstation

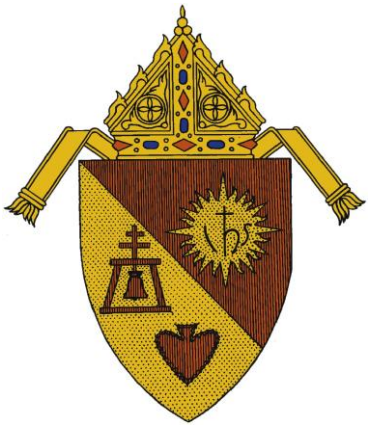
Personal Use: Personal use of a computer is defined as using a computer that is outside the scope of that person's job description, with the exception of work assigned by their direct supervisor.

Remote Computer Services: Computer services that are part of the organization's data processing and can be accessed only through a wide-area-network, the Internet or modem.

Virus: A segment of replicating computer code that attaches itself to application programs or other executable system components. These code segments copy themselves and spread from program to program and from computer to computer.

WAN (**Wide-Area-Network):** A long-distance network distributed geographically but connected via telecommunication links.

Workstation: A personal computer that performs local processing and network services.



COMPUTER POLICIES

I HAVE RECEIVED THE Diocese of San Bernardino Computer Polices, effective date of September 1st, 2010.

I understand that these policies represent the general guidelines for computer use by employees and seminarians of the Diocese of San Bernardino and that I must abide by them as a condition of employment.

I acknowledge that the document contains, but is not limited to, the following policies: electronic communications, scheduler usage, and software use.

I understand that the policies may change. I also understand that it is my responsibility to address questions or request clarifications about the Computer Policies to the Director of Information Services AND the Director of Human Resources.

Please Print:

_____ _____

Name Office

Please Sign:

_____ _____

Name Date