Diocese of Shreveport

Policy on the Use of Computer, Internet, E-Mail and Communication Media

Vision Statement

With a treasure, a truth, a love that is communicated in ways that honor God and that inspire, challenge and sanctify all people, the Diocese of Shreveport communicates and evangelizes by using modern communication technologies to promote the Gospel values of the Roman Catholic faith. We seek to educate and enrich lives by challenging them to a deeper understanding of official Church teachings, the ethical use of technology, a greater commitment to the practical applications of those teachings and the growth and development of the human person, the human family, and society in general.

Statement of Purpose

The policies and procedures presented herein apply to all Diocesan personnel, Church parish staff members (full-time, part-time and temporary/volunteers), students, faculty, library patrons, as well as those associated with church organizations. These policies will address standards for utilization of Diocesan electronic media and security.

This policy supersedes the previous communication policy referred to in the Employee Handbook dated October 1, 2011, and states minimum requirements for all diocesan locations. The Diocese of Shreveport (DOS) reserves the right to amend or revise this document, in whole or part, at any time. The Diocese of Shreveport's Moderator of the Curia will provide written notification of any change.

Diocesan Property

Electronic communications systems provided by the Diocese of Shreveport (DOS) including, but not limited to computer systems, internet, voice mail, telephones, social media, electronic mail, blog, fax and all messages, and documents and copies generated on or handled by these electronic communications systems, including back-up copies, are considered to be the property of the Diocese of Shreveport.

Authorized Usage

As a productivity and educational tool, the Diocese of Shreveport (including all parishes and schools) provides and encourages the use of electronic communications in conducting Diocesan business. The Diocese of Shreveport (DOS) encourages its users to be mindful of the purpose and consistency in the mission of the Church in its public image. Users must ensure that their conduct, whether official or unofficial, in social media environments, blogs, email, and the Internet, conforms to the teachings of the Catholic Church. The Diocese of Shreveport's electronic communications systems must be used solely to facilitate the mission of the Diocese. Users are encouraged to limit the personal use of Diocesan electronic communication systems to emergencies or when extenuating circumstances so warrant. Diocesan electronic communication systems are not to be used for private business activities, social networking or amusement/entertainment purposes. If personal electronic devises must be used for diocesan business, employees are asked to password protect these devices and to hold usage to a minimum. Users are reminded that the use of Diocesan electronic communications resources should never create either the appearance or the reality of inappropriate use. Inappropriate use or any attempt to violate, circumvent and/or ignore these policies may result in loss of access privileges and disciplinary action, up to and including termination.

Waiver of Privacy Rights

Users expressly waive any right of privacy to anything they create, store, send or receive using any device that connects to or accesses the DOS's communication system. By accessing DOS communication systems, users consent to allow the Diocese access to and review all materials created, stored, sent or received by the user through the DOS network or internet connection at any time and without prior notice.

Use of Internet and Email

Users must ensure that their actions do not reflect adversely on the Diocese. Therefore, users provided with access to the Internet and the services provided through the connection offered by the Diocese of Shreveport (DOS) have the following responsibilities.

The internet connection provided by the Diocese is not to be used to knowingly submit, publish, transmit, or display messages or images of a defamatory, inaccurate, morally inappropriate, abusive, obscene, profane, sexually oriented, threatening, cyberbullying, racially offensive or otherwise illegal material. In addition, Diocesan communication resources may not be used to solicit for private advertising, personal commercial business or to benefit any organization not affiliated with the Diocese.

Electronic Communications Monitoring

Electronic communications will not be monitored by the DOS as a standard practice. However, by using the electronic communications resources provided and owned by the DOS, employees agree to the interception of any electronic communications when activities are called into question.

Internet usage (sites visited, permitted) is monitored. Users are cautioned that many web sites include offensive, sexually explicit, and inappropriate material and may circumvent filters established to protect them. In general, it is difficult to avoid at least some contact with this material while using the Internet. Additionally, having an email address on the Internet may lead to receipt of unsolicited email containing offensive content. Users accessing the Internet do so at their own risk and the DOS is not responsible for unauthorized materials viewed or downloaded by users from the Internet. To minimize these risks, your use of the Internet in the DOS is governed by the following policy:

- All messages and related files are property and records of the DOS. Users should not assume electronic communications are totally private and confidential.

- The DOS also reserves the right, in the discretion of the diocesan bishop, to review any employee's or user's electronic files and 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 DOS policies. There may also be other business or legal reasons for the DOS to access or disclose any employee's electronic files or messages.

Violation of Network Security

The DOS users must respect the confidentiality of other people's electronic communications. Users may not attempt to "hack" into other systems, use other people's login IDs without authorization, "crack" passwords, breach computer or network security measures, monitor electronic files or communications of other patrons or third parties except by explicit permission by supervisors or department directors.

The DOS restricts access to its computing resources, and requires that users identify their accounts with a username and password. With the exception of the Information System Department, sharing your account security with others is prohibited, with the exception that user id(s) and password(s) for all voice mail, web sites and software involved in performing and maintaining the work of diocesan departments will be shared with the department supervisor or department director. The information Systems Department does not keep lists of any user security information.

If users need to share computer data, they should utilize message forwarding, shared network server folders, and other authorized file-sharing media. Users should be aware that cloud storage (i.e. Dropbox, Carbonite, etc.) services are not governed by regulations or certifications such as, HIPAA or RPC, etc., but do comply with basic security and privacy rules. Use of these services should be *restricted to personal data and documents only.* Never save Diocesan data, documents or information to online storage sites. Cloud storage accounts set up for personal use on Diocesan computers should be done through the Information Systems department. The user's Diocesan email account and password will be used to set up this account and will be maintained by the supervisor or department director as well as the Information Systems department.

No email or other electronic communication may be sent which attempts to hide, misrepresent or obscure the identity of the sender.

Deliberately violating system security, attempting to violate system security, and exploiting holes in system security on any DOS system are prohibited and will not be tolerated. If you do find a hole in the security of any DOS system, notify Information System Department immediately.

Communications Systems Management

Users granted access to the DOS email system is given a limited space for email storage. Messages no longer needed for Diocesan purposes must be periodically purged from Outlook email by the user.

To maximize server storage and minimize backup times, personal photos, videos or documents should never be saved on the server. Server storage is strictly reserved for Diocesan related business information and systems only.

Social Networking or Social Media

The DOS understands the current popularity of social networking websites, Facebook, Twitter, MySpace, or comparable sites. It also understands that employees may choose to visit or use such sites while not at work and while not using the Diocese's equipment or networks. All Diocesan employees play an integral role in its image and customer service and every employee functions as a representative of the Diocese. The DOS has a legitimate interest in ensuring that no employee exposes the Diocese, him or her to embarrassment or liability while using any social networking website while using the Diocese's network or during personal time. Employees should keep in mind that such websites, by their very nature, are public. As such, all employees are encouraged to use such websites responsibly and to avoid any activity that may be deemed offensive or otherwise inappropriate. Employees are discouraged from participating in any activity that may cast him or her, or the Diocese, in an embarrassing or negative light. Employees are prohibited from engaging in any activity intended to degrade an employee or the Diocese in society or that may bring an employee, the Diocese or any of the Diocese's facilities into public disrepute, contempt, scandal or ridicule. Employees are further prohibited from using, revealing, posting, or including any information regarding the Diocese, or clients, or any confidential or private information of employees, on any social networking website.

Use of personal social network accounts and personal user IDs for company use is prohibited. An employee needing access to social networking sites to conduct Diocesan business should submit a request to the Information Systems department (IS) for access through their supervisor or department director.

If access approved IS will create a user ID on the targeted social network using the employee's Diocesan email address and will communicate the initial account password to the employee. The login information and any password change(s) will be maintained by the requesting supervisor and/or department director as well as the IS department.

Use of Diocesan social network user IDs for personal use is prohibited. Examples of prohibited use of Diocesan user IDs include downloading and installing plug-ins or helper applications such as those that try to access the Diocese's email directory, joining groups using a Diocesan user ID for personal reasons or adding personal friends to an employee's friends list.

Creation of "groups" within the social network to support Diocesan goals is allowed. However, supervisors and/or department directors requesting access will regularly monitor and moderate group activity. It is the responsibility of the supervisor/department director to monitor individual group member activity as well as to ensure Diocesan use of the social network complies with the social network's Terms of Service (TOS) or Terms of Use (TOU), as applicable.

Telephone System

The Diocese recognizes that there may occasionally be times when personal calls must be made or received during business hours. Such calls should be held to emergency situations or when extenuating circumstance so warrant, and must not interfere with the employee's work. Employees are encouraged to make such calls during their breaks or at lunchtime.

When a personal long-distance call results in a charge, the employee is responsible for the billed charges and must reimburse the Diocese for the charges. The Diocese 800 number is reserved for Diocesan use only. Business phone calls should be made using diocesan equipment rather than personal devices, unless circumstances cannot accomodate use of diocesan systems.

Smart Phones, Tablets

Smart phones, tablets, or other electronic devices applies to any device that makes or receives phone calls, leaves messages, sends text messages, and allows for the reading of and responding to Diocesan email whether the device is Diocese-supplied or personally owned.

Employees are asked to password protect smart phones, tablets or any electronic device in which Diocesan information is stored, sent or received.

Use of personal cell phones must be held to a minimum and must not interfere with the employee's work. Employees are encouraged to make personal calls during their breaks or at lunchtime.

Software

It is a violation of DOS policy for any employee, including system administrators and supervisors, to use outside materials (games, disks, personal software) on DOS desktops and laptop computers or connect personal computers or laptops to Diocesan network resources without prior permission.

The DOS strictly follows all software licensing agreements. Therefore, users are prohibited from installing software on Diocesan laptops, desktops or servers without prior permission. Proof of licensing will be required.

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.

Frivolous Use

Computer and network resources are not unlimited. Network bandwidth and storage capacity have finite limits, and all users connected to the network have a responsibility to conserve these resources. As such, the users must not deliberately perform acts that waste network resources or unfairly monopolize network resources to the exclusion of others. These acts include, but are not limited to, sending mass mailings or chain letters, spending any amount of time that interferes with work on the Internet, social media, playing games, engaging in online chat groups, excessive streaming audio and/or video files (i.e., radio and/or movies), or otherwise creating unnecessary loads on network traffic associated with non-business-related uses of the Internet.

Virus detection

Files obtained from sources outside the Diocese, including disks or flash drives brought from home, files downloaded from the Internet, newsgroups, bulletin boards, files attached to email, or files provided by patrons or vendors, may contain dangerous computer viruses that could damage the Diocese's servers or computers. Users should never download files from the Internet, except for Diocesan related work, email from individuals they know and are expecting the attachment or use disks from non-Diocesan sources, without first scanning the material with Diocesan-approved virus checking software. If you suspect that a virus has been introduced into the Diocese's network or the user's computer, notify the Information Systems Department immediately.

Fax

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.*

UTILIZATION OF ELECTRONIC COMMUNICATIONS

User Agreement

I have been apprised of the Diocese's Policy on the Use of Computer, Internet, Email and Communications Media (Use Policies), and I am requesting the following electronic communication resources:

- ✓ Electronic Mail (email)
- ✓ Internet Access
- ✓ Telephone System
- ✓ Electronic/digital files

I acknowledge the following:

- I have read and understand the **Use Policies** set forth by the Diocese of Shreveport.
- I understand that access provided by the Diocese's internet, email, telephone and other forms of electronic access is for the benefit of the Diocese of Shreveport.
- I understand that internet access is provided for the mission, business and educational purposes and that the Diocese of Shreveport has taken precautions to eliminate and/or control access to controversial material by monitoring internet access traffic. I recognize it is impossible for the Diocese of Shreveport to restrict access to all controversial and inappropriate materials. I will not hold the Diocese of Shreveport, its employees, agents, or Board members, liable for any harm caused by unauthorized materials or software obtained via the Internet.
- I have read and agree to comply with the terms of this policy governing the use of Diocese of Shreveport's electronic communication systems. I understand that violation of this policy may result in my privileges being revoked and disciplinary action, including possible termination and/or appropriate legal action may be taken.

_____ _____

Signature Date

_____

Name (print)