DIOCESE OF DALLAS

Pastoral Center

Computer Systems, Internet Usage and Security Policy

Diocese of Dallas Pastoral Center
Computer Systems, Internet Usage and Security Policy

The purpose of this policy is to outline the acceptable use of computer equipment and technology resources at the Pastoral Center of the Diocese of Dallas Pastoral Center. These rules are in place to protect the employee and the Diocese of Dallas Pastoral Center. Inappropriate use exposes the Diocese of Dallas Pastoral Center to risks including virus attacks, compromise of network systems and services, and legal issues.

1. General Use and Ownership

A. The equipment, services, and technology provided remain at all times property of the Diocese of Dallas Pastoral Center. All information stored, transmitted, received, composed or contained in the Diocesan Information System is the property of the Diocese.

B. For security and network maintenance purposes, authorized individuals within the Diocese of Dallas Pastoral Center may monitor equipment, systems and network traffic at any time.

C. Employees are expected to limit their computer use to Diocesan business related issues. Appropriate, reasonable, personal use will be allowed during the employee's personal time, such as lunch hours and/or before and after the normal workday excluding the use of the wireless network. Employees are responsible for exercising good judgment regarding the reasonableness of personal use.

D. For security reasons, only **Diocesan owned equipment** may be connected to the Diocesan network (wired or wireless) using staff login credentials (does not apply to approved SSLVPN Connections). Non-Diocesan owned devices should only connect to the Diocesan provided internet via the "Guest" wireless login and passcode.

E. **The primary location for storing all Diocesan files is on the Diocesan network**. Users are responsible for management of network directories under their purview. Each user shall review the contents of his/her directory at least once every six months to remove extraneous material.

F. No personal equipment, such as printers, scanners, or other equipment is permitted to be connected to the Diocesan network or other Diocesan technology resource.

G. Standard equipment configurations should not be changed.

H. For security and network purposes users will not be given administrative rights to the local pc without an authorization form signed by both department head and senior staff including a statement of need for access. All software, hardware and updates will be maintained by the Business Office Information Technology Division and performed as needed.

2. Internet and Email Usage

A. All activities must be appropriate, presenting a positive, professional image of both the employee and the Diocese of Dallas Pastoral Center. Data that is composed, transmitted, accessed or received via the Internet must not contain content that could be considered discriminatory, offensive, obscene, threatening, harassing, intimidating or disruptive to any employee or other person.

B. Users must ensure that their conduct in public forums, email, and the Internet conforms to the teachings of the Catholic Church.

C. The unauthorized use, installation, copying or distribution of copyrighted, trademarked, or patented material on the Internet is expressly prohibited.

D. All users connected to the network have a responsibility to conserve computer resources such as bandwidth and storage capacity. The user must not deliberately perform acts that waste computer resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, sending mass mailings or chain letters, spending excessive amounts of time on the Internet, playing games, engaging in online chat groups, uploading or downloading large files, *accessing streaming audio and/or video files, or otherwise creating unnecessary loads on network traffic associated with non-work-related uses of the Internet.*

E. The Diocese of Dallas Pastoral Center Business Office Technology Division reserves the right to review, audit, intercept, access and disclose all messages created, received or sent over the electronic mail system for any purpose. Employees should have no expectation of privacy in anything they create, store, send or receive using the Diocese's computer equipment or network system. The use of encryption of information is recommended when possible.

2.1 Social Networking Sites:

A. Abide by Diocesan guidelines as spelled out in the ***Diocese of Dallas Social Media Policy*****.** Social Media Policy

3. Remote Access

A. *Remote Email Access*: The user is expected to safeguard their Diocesan email account when accessing it through the internet from a remote location. All items addressed and implied in this document also apply to accessing email accounts remotely.

B. When accessing email via a personally owned mobile device:

1. Mobile computing and storage devices include, but are not limited to, the following: laptop computers, personal digital assistants, plug ins, USB port devices, CD's, DVD's, flash drives, modems, handheld wireless devices, wireless network cards, mobile phones, mobile smart phones, digital tablets, and any other existing or future mobile computing or storage device.
2. User agrees to ensure the adequate physical security of the device.
3. User agrees to maintain the software configuration of the device – both the operating system and the applications installed.
4. **User agrees to prevent the storage of sensitive company data in unapproved applications on the device.**
5. User agrees to immediately notify the Pastoral Center Business Office Technology Division of a lost or stolen device.
6. User agrees to enforced phone screen lock password requirement (The Diocese does not track that password. It is the user's responsibility to maintain that password as the Diocese does not control the resetting of passwords on the personally owned device.)
7. User agrees to not use the mobile device for business related conversations or texting while driving.

8. **Personal smartphones are not centrally managed by the Pastoral Center Business Office Technology Division. Therefore, any support need or issue related to their device is the responsibility of the owner.** *Specifically, the user is responsible for:*

   a) *Settling any service or billing disputes with the carrier*
   b) *Purchasing any required software not provided by the manufacturer or wireless carrier*
   c) *Device registration with the vendor and/or service provider*
   d) *Maintaining any necessary warranty information*
   e) *Battery replacement due to failure or loss of ability to hold a charge*
   f) *Backing up all data, settings, media and applications*
   g) *Installation of software updates/patches*
   h) *The device will be used in a manner consistent with the Computer Usage Security Policy*
   i) *The Diocese of Dallas Pastoral Center Business Office Technology Division reserves the right to, at will, monitor corporate messaging systems and data including data residing on the user's mobile device*
   j) *The Diocese of Dallas Pastoral Center Business Office Technology Division reserves the right to, at will, remotely modify, including remote wipe or reset to factory default, the users' mobile device configuration*

C. *SSLVirtual Private Network (SSLVPN) Access*: The Diocese of Dallas Pastoral Center provides remote connectivity to select users. Those staff utilizing this tool must confirm the remote computer utilizes an up to date and operational Firewall and Anti-Virus application. The SSLVPN should be used from only one remote computer and that computer location must be prior approved by a Diocesan Staff Director. All items addressed and implied in this document also apply to SSLVPN Connectivity.

D. *Diocesan equipment* transported outside of the designated workspace should be used for Diocesan business only. General Use and Ownership Policy apply in this instance.

4. Security:

A. All Employees of the Diocese of Dallas Pastoral Center agree to participate in regular Security and Internet usage training classes. Courses will be assigned to staff at a minimum of two times per year and randomly throughout the year when new security issues arise or as needed based on user activity. All training courses are mandatory and required to be taken within time frame allotted.

B. The Diocese of Dallas Pastoral Center requires complex passwords. Passwords can only be changed one time per day and a previous password cannot be used again for 10 times. Passwords will expire after 90 days. It is the employee's responsibility to change the password in a timely fashion as to not let it expire. A complex password is 8-10 characters in length and must contain at least three of these four types of characters.

1. Upper Case Letters
2. Lower Case Letters
3. Numbers
4. Symbols

C. The Diocese of Dallas Pastoral Center restricts access to its computing resources and requires that users identify their accounts with a username and password. Sharing user accounts with persons other than Business Office Information Technology Division Staff is prohibited. If there is a breach with user accounts and/or passwords, it will be traced back to the employee and the employee will be held responsible.

D. The employee must safeguard their network connection. Steps should be taken to set computer to “Locked” or "Standby" mode if the employee will be away from their computer for an extended length of time. A username and password must be entered for the computer to become operational again from the Stand-by mode. The employee must log off of the network when leaving their computer for the workday.

E. Users must follow the below general practices as simple preventative measures against viruses:

a. Never open any files or macros attached to an email from an unknown, suspicious, or untrustworthy source.

b. Delete attachments to emails that are from unknown, suspicious or untrustworthy source immediately, and then empty them from your Recycle Bin/Trash/Deleted Items folder.
c. Delete spam, chain & other junk email.
d. Never download files from unknown or suspicious sources.
e. Always scan any portable media for viruses before using it.

F. Violations of this policy, including breaches of confidentiality or security, may result in suspension of electronic communication privileges and disciplinary action up to and including termination and civil and criminal penalties under state and federal laws.

Diocese of Dallas – Pastoral Center
Computer Systems, Internet Usage and Security Policy
Acknowledgement Form

I have read the Diocese of Dallas Pastoral Center Computer Systems, Internet Usage and Security Policy, as it applies to the paid or volunteer position I hold in the Diocese of Dallas Pastoral Center:

I fully understand the terms of this policy and agree to abide it. *I realize that the Diocese may record for management use any action I take on a Diocesan or parish network, device or computer. I acknowledge that any document, program, database, graphic or other digital production that I may create on said equipment is the property of the Diocese of Dallas Pastoral Center.* I acknowledge that any violation of this policy will incur disciplinary action up to and including dismissal or possible criminal prosecution.

I agree to comply with these and all other related Diocesan policies:

Signature	Date
Printed Name	Department

This document will be placed in the employee's or volunteer's personnel file in Human Resources.