Diocese of Des Moines
Computer Usage and Security Policy

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

1. General Use and Ownership

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

For security and network maintenance purposes, authorized individuals within the Diocese of Des Moines may monitor equipment, systems and network traffic at any time.

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.

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 VPN Connections). Non-Diocesan owned devices should only connect to the Diocesan provided internet via the "Guest" wireless login and system generated passcode.

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.

No personal equipment, such as printers, scanners, or other equipment is permitted to be connected to the Diocesan network or other Diocesan technology resource without prior authorization by the Technology Department.

Standard equipment configurations should not be changed.

2. Internet and Email Usage

All activities must be appropriate, presenting a positive, professional image of both the employee and the Diocese of Des Moines. 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.

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

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

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.

The Diocese of Des Moines 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. The use of encryption of information is recommended when possible.

Social Networking Sites:

The accessing of social media sites is permitted for business related purposes. Two primary values should be followed when using social media: 1) Visibility and 2) Accountability.

Diocesan sites require adherence to these guidelines:

1) Do not use Diocesan email addresses to register on social networks, blogs or other online tools utilized for personal use.
2) Passwords and names of sites should be registered in a central location within the department managing the site with more than one Diocesan staff member having access.
3) Abide by Diocesan guidelines as spelled out in the Computer Usage and Security Policy.
4) Personal communication reflects the Church.
5) Write in first person. Do not claim to represent the official position of the organization or the teachings of the Church, unless authorized to do so.
6) Identify yourself.
7) Abide by copyright, fair use & disclosure laws.
8) Do not divulge confidential information to others.
9) Do not cite others, post photos or videos, link to other's material, without their approval.
10) Obtain parental permission of a minor before communicating with them via social media. Provide parents the opportunity to be copied on all material sent to their children via social media (includes text messages). No employee should initiate the "friending" of a minor. Minors must make the initial request.
11) Diocesan social networking sites should be regularly updated. As with any ministry effort, there should be an intentional plan and a set of goals regarding establishing and maintaining a web presence.
12) There should be no expectation of privacy.
13) Personal Social Media sites should also reflect Catholic values.
14) Report "unofficial" sites that carry the Diocesan logo to the Diocesan Communications Office.

3. Remote Access

i. 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.

ii. 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 Diocesan Technology Department 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 Diocese Technology Department. Therefore, any support need or issue related to their device is the responsibility of the owner.

   Specifically, the user is responsible for:
   - Settling any service or billing disputes with the carrier
   - Purchasing any required software not provided by the manufacturer or wireless carrier
   - Device registration with the vendor and/or service provider
   - Maintaining any necessary warranty information
   - Battery replacement due to failure or loss of ability to hold a charge
   - Backing up all data, settings, media and applications
   - Installation of software updates/patches
9. The device will be used in a manner consistent with the Computer Usage Security Policy
10. The Diocese reserves the right to, at will, monitor corporate messaging systems and data including data residing on the user's mobile device
11. The Diocese reserves the right to, at will, remotely modify, including remote wipe or reset to factory default, the users' mobile device configuration

iii. Virtual Private Network (VPN) Access: The Diocese of Des Moines 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 VPN software is to be loaded to 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 VPN Connectivity. (See Attachment A.)

iv. 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:

The Diocese of Des Moines 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 the Technology Department 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.

The employee must safeguard their network connection. Steps should be taken to set computer to "Stand-by" 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.

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

1. Never open any files or macros attached to an email from an unknown, suspicious, or untrustworthy source.
2. 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.
3. Delete spam, chain & other junk email.
4. Never download files from unknown or suspicious sources.
5. Always scan any portable media for viruses before using it.

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.

ATTACHMENT A

Virtual Private Network (VPN) Access Application

The Diocese of Des Moines provides remote connectivity to select users. Those staff utilizing this tool must agree to exclusively utilize the Diocese provided FortiClient Firewall/Antivirus/Antispyware software application on their remote (home) computer. The VPN software is to be loaded to only one remote (home) computer and that computer location must be prior approved by a Diocesan Staff Director. The VPN software can not be copied or distributed by the select user.

Name: _____

Department: _____

I wish to utilize the VPN remote connectivity technology. I will state below the reasons for needing this remote access, how I will use this access, and information regarding the location of the remote computer that I will use to connect to the Diocesan network.

_____

_____

_____

_____

_____

_____

_____

_____

_____

Signature & Date: _____

Department Director's Approval Signature: _____