APPLICATION

The provisions of this policy shall apply to all employees of the Roman Catholic Diocese of Covington ("Diocese"). Accordingly, any reference to the Diocese is to be interpreted to mean any Diocesan parish, school, institution or its employees. Any reference to employees is to be interpreted to mean any employee of a parish, school or institution of the Diocese of Covington. Any variation or deviation from this policy requires the approval of the Bishop or Vicar General of the Diocese.

The policy has been created to protect both the Diocese and its employees. Any violation of this policy is considered grounds for disciplinary actions up to, and including, termination of employment.

RESPONSIBILITIES

Role	Responsibilities
Information Technology (IT) Personnel	Responsible for interpreting and monitoring compliance with this policy.
Pastors, Parochial Vicars, Pastoral Administrators, Principals and Administrators	Responsible for determining the types of voice and data technology required for their employees to fulfill their job responsibilities. Responsible for ensuring that employees are utilizing these services in accordance with the provisions of this policy.
Employees	Responsible for understanding and complying with this policy.

COMPUTER HARDWARE AND SOFTWARE

All acquisitions of computer hardware and software must be processed through IT Personnel. Computer software is normally licensed only to a single computer. Therefore:

- Diocesan provided software may not be duplicated other than for backup purposes
- Only IT personnel may install or move software on Diocesan-owned computers
- Except for software approved by the Diocese, no other software may be used or installed on Diocesan-owned computers.

Employees who do not follow these requirements may expose themselves and the Diocese to criminal charges as well as civil liability for copyright violations. Any employee who becomes aware of installed software packages on Diocesan computers that does not meet the above requirements, must report such situations to their Director or IT Personnel. Employees shall contact IT Personnel for advice or assistance in unplugging, disconnecting, or moving computer equipment.

DIOCESAN ISSUED EQUIPMENT

Employees may be required to use Diocesan equipment (hardware, software, electronic and voice mail) in the execution of their duties. Only Diocesan computers are to be used for work-related tasks. Any work-related information that is to be processed, stored, or transmitted must be done on Diocesan equipment. If in doubt, employees are to check with their Director or IT Personnel.

For security purposes and the protection of the Diocese, Diocesan laptops must be secured when not in use by the employee. Laptops shall never be left on a desk at the end of the working day, and must be secured or taken home by the relevant Diocesan employee. When left in an unattended car, laptops should be stored out of sight and car or trunk locked. Mobile phones, tablets, and any media devices containing sensitive information shall be securely stored when not in use. All devices with access to work related information must be password protected (i.e. phones and laptops must require a password to access the device) to prevent misuse if lost or stolen.

PERIODIC AUDITS

While the Diocese desires to provide a reasonable level of privacy, users should be aware that any data created on the Diocesan networks and systems remain the property of the Diocese. Because of the need to protect the Diocese's network, management cannot guarantee the confidentiality of information stored on any network device belonging to the Diocese. The Diocese reserves the right to monitor all systems, software installations and usage of its networks. IT Personnel will conduct periodic audits to ensure compliance with this policy. Unannounced, random spot audits may be conducted as well. During such audits, scanning and elimination of computer viruses and unnecessary files (e.g. unauthorized pictures, sound files, etc.) may be performed. Other unsanctioned software may also be uninstalled at this time.

PERSONAL EQUIPMENT

Employees may not use their own personal equipment on the Diocesan network. Employees may not use their own personal equipment to store, process or otherwise manipulate Diocesan data, information, records or software. Any storage device that is to be connected to the Diocesan network must be scanned by IT for viruses prior to connection.

VIRUS PROTECTION

A virus is potentially malicious programming code that will cause some unexpected or undesirable event. Viruses can be transmitted via e-mail, or instant messaging attachments, downloadable internet files, flash drives, CD's, DVD's, etc. Viruses are usually disguised as something else, making their presence not obvious to the computer user. A virus infection can be very costly to the Diocese in terms of lost data, lost staff productivity, and/or reputation.

All files downloaded to local hard or removable drives will be automatically scanned for viruses by the antivirus software. If unforeseen circumstances prevent automatic scanning, IT will provide instructions for manually scanning files.

Virus protections software shall not be modified by anyone without the approval of IT Personnel.

If an employee receives what he/she believes to be a virus, or suspects that a computer is infected with a virus, it must be reported to IT Personnel immediately. The employee should stop using the infected computer and report the following information (if known): virus name, extent of infection, source of virus, and potential recipients of infected material.

Information about viruses detected on Diocesan computers must not be communicated outside of the Diocese. If a virus is detected in a file sent by a sponsor, as a courtesy, the Diocesan IT Personnel will notify the sponsor and ask them to resend the file.

COMPUTER ACCOUNTS AND PASSWORDS

The Diocese allows access to computing and communications resources to full and part-time employees, volunteers, contract workers and business partners. The Diocese reserves the right to withdraw such privileges pursuant to contract stipulations as well as actions spelled out by our acceptable use policies and other policies that govern employee and contractor relations.

Individual computer accounts are created by IT Personnel for the exclusive use by the individual for whom the account was created. This includes network accounts, e-mail accounts, and accounts created for accessing applications. Individual computer accounts may only be used by the employee for whom the account is created.

Employees must not share their account passwords with anyone except their Director if requested. Directors may not share an employee's password with anyone else, and are to only request an employee's password at the time of the employee's termination of employment, or to review information that is exclusively held by the employee. If a Director wants to review the information held by an employee, the Director must first contact IT to determine if IT can grant the Director access to the information without the employee's password.

Employees are responsible for changing their password on a periodic basis as required by technology standards. Current standards require a password to be changed every 90 days. Employees must use complex passwords that are difficult for others to guess. Employees must not document their passwords or share them with other employees.

PRIVACY AND CONFIDENTIALITY

Information contained on the Diocesan systems is to be considered confidential. Examples of confidential information include, but are not limited to: employees personal information, donor lists, parishioner information, and donor information. Employees should take all necessary steps to prevent unauthorized disclosure of any information that could be harmful to Diocesan employees or to the Diocese's reputation. Distribution of any confidential information must be approved by the Bishop or Vicar General of the Diocese.

Diocesan software, documentation, and all other types of internal information must not be sold or shared with anyone for any reason.

The Diocese reserves the right to examine electronic mail, directories and file, and other information stored on Diocesan computers, tapes, disks and to remove/modify the hardware/software to conform to Diocesan standards.

Electronic mail and internet accounts are the exclusive property of the Diocese. Under no circumstances are Diocesan employees allowed to create, receive, access, or send personal communication from the Diocesan electronic mail or internet system.

Employees should treat e-mail messages and internet records as shared paper files, with the expectation that anything in them is available for review. The Diocese reserves the right to access, retrieve, read and delete any communication created, received or sent through the Diocesan electronic mail system or from the Diocese internet account, including sites visited, without notice. Therefore, it is important that employees conduct only work related activities with the equipment as described.

By using the e-mail system, employees users expressly consent to the Diocesan monitoring policy, agree to comply with all limitations on the use of the e-mail system and understand the e-mail system is not a private communication medium.

The use of authorized passwords by employees should not be construed as creating a private communication medium. In the interest of security, this policy requires that employees treat their passwords in a confidential manner. Employees shall never be asked nor should they submit their network password to anyone, except their Director in the circumstances addressed in §2.3 above. Every effort must be made to protect and treat all Diocesan information assets as confidential. Employees may not publicly disclose via the internet (or any form of electronic communication) inappropriate information regarding the Diocese.

Diocesan confidential, proprietary, or secret information must not be sent via electronic mail or over the internet unless it has first been protected through the use of strong encryption techniques by a method approved by IT Personnel.

ELECTRONIC AND VOICE MAIL

All forms of electronic and voice mail provided by the Diocese are exclusively for Diocesan business use and are not to be used for personal business of any kind.

Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, or malicious code that could harm the Diocesan systems, networks or reputation.

Never send confidential (credit card numbers, sensitive documents) or personally identifiable information (social security, date of birth, etc.) via e-mail unless it has been approved by management and is secured using Diocesan approved encryption.

No e-mail messages should be created or sent which may constitute intimidating, hostile, or offensive material. The Diocesan policy against harassment of any kind, applies fully to the e-mail and voicemail system. Any violation of the harassment policy is grounds for disciplinary action up to, and including, termination of employment.

The email system should not be used to solicit outside business ventures, political, or other personal causes by an employee. The Diocese employees' email addresses shall be used for business purposes only and shall not be used to subscribe to non-business related websites or mailing lists.

Unsolicited mail is unwelcome and should simply be deleted by the employees in cases where the message is able to circumvent the Diocesan spam filtering tools. If this occurs frequently, please contact IT Personnel.

Urgent or time sensitive communication should not be exclusively sent via email. Such communication should also be sent via an alternative method (postal service, phone call, etc.) to ensure the recipient receives the information.

Proper business etiquette should be maintained when communicating via email. When writing messages, employees should be clear and concise. If a message requires an action by the recipient(s), a follow up date should be provided. Verbal attacks, sarcasm, poor language, inappropriate comments, etc. are to be avoided. When communicating via e-mail, there are no facial expressions and voice tones to assist readers in determining the meaning or intent behind a comment, which leaves room for misinterpretation. Therefore, e-mail should resemble typical professional business correspondence and should be respectful in tone and nature.

Employees should be cognizant that using the "forward" option on messages with attachments will re-send the attachment to the originator. The attachment should be manually deleted by the sender, unless it is the intention of the sender for the recipient to get the attachment. Additionally, sending large attachments take a considerable amount of time to send. If a project or assignment requires frequent sending of messages with large attachments, please notify IT Personnel for alternative methods of sharing large files with user groups.

Retaining messages consumes a considerable amount of disc space. While it is important to keep messages that are important to projects and job duties, users should delete messages when they are no longer of value.

Mailing lists provide convenient and affective communication to target groups within the Diocese. However, employees should be cautious when using them to minimize unnecessary mail traffic to unconcerned parties. Using the "reply to all" feature to mailing list should be kept to a minimum. Personal items are not to be sent to mailing lists.

Any personal long-distance calls that must be made (except toll-free calls) should be charged to the employees' home telephone, personal credit card, personal calling card or be charged to the called party. If a personal long-distance call must be made that will be billed to the Diocese, the employee should receive permission from a Director prior to making the call.

Where legally allowed, the Diocese, reserves the right to monitor telephone and voice mail use, including telephone conversations, and the contents of voicemail boxes. Monitoring of telephone and voicemail use will only be done for legitimate reasons, such as to assess customer service quality assurance, retrieve lost messages, recover from system failure, or comply with investigations of wrongful acts.

INTERNET UTILIZATION

Any Diocesan paid subscription to internet access services must be approved by the employee's Director, Vicar General, or the Bishop. Internet usage is to be restricted exclusively for Diocesan business use. Employees are not to use any diocesan network or internet services for personal business at any time.

Appropriate Use

Diocesan employees are encouraged to use the internet to further the goals and objectives of the Diocese. The types of activities that are encouraged include:

- Communicating with fellow employees, business partners of the Diocese and clients within the context of the employee's assigned responsibilities;
- Acquiring or sharing information necessary of related to the performance of employee's assigned responsibilities;
- Participating in educational or professional development activities

Inappropriate Use

Individual internet use must not interfere with others' use of the internet. Users are not to violate the network policies of any network accessed through their account. Internet use at the Diocese will comply with all federal and state laws, as well as all Diocesan policies and contracts. Users 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 emails or chain letters, subscribing to or participating in non-business related mailing lists or online "chat groups" or "streaming" internet radio/TV programs, watching/downloading streaming video or otherwise creating unnecessary network traffic or spending excessive amounts of time on the internet. Because audio, video and picture files require significant storage space, files of this sort may not be downloaded and/or stored unless they are business-related.

The use of peer-to-peer telephony (Skype) and/or file sharing programs (such as Kazaa, BitTorrent, LimeWire or Bearshare), is expressly prohibited unless required and approved for Diocesan activities.

Other prohibited activities include but are not limited to, the following:

- The Internet must not be used for inappropriate or unlawful purposes, including, but not limited to, copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, Impersonation, illegal gambling, soliciting for illegal pyramid schemes, and computer tampering (e.g. spreading computer viruses).
- The Internet must not be used in any way that violates Diocesan policies, rules, or administrative orders. Use of the Internet in a manner that is not consistent with the mission of the Diocese, misrepresents the Diocese, or violates any Diocesan policy is strictly prohibited.
- Individuals shall not access the internet for their personal use. The Diocese prohibits unauthorized, unsolicited mass emailing, access of Diocesan resources or network facilities by non-employees, competitive commercial activity and the dissemination of chain letters.
- Individuals must not view, copy, alter, or destroy data, software, documentation or data communication belonging to the Diocese or another individual without authorized permission.

- In the interest of maintaining network performance, users shall not send unreasonably large electronic mail attachments.
- Employees must not download and/or attempt to the installation of any application downloaded from the Internet without prior approval from IT Personnel.
- Credit Cards numbers, telephone calling card numbers, log-in passwords, and personally identifiable information which can be used to gain access to goods or services must never be sent via email unless encrypted by a method approved by IT Personnel.
- The Diocese is responsible for any information posted to, or made available via the internet, in the Diocese's name. Accordingly, such information is to be approved prior to posting.
- Employees shall not engage in any blogging or newsgroup activity that may harm or tarnish the image, reputation and/or goodwill of the Diocese or its employees.
- Unless expressly approved, employees shall not disclose Diocesan information in blogs or newsgroups, nor shall employee's login to, or sign on to, such services using a Diocesan email address. Doing so may give hackers an advantage when trying to steal data or breach the network.

MONITORING AND FILTERING

The Diocese reserves the right to monitor any activity occurring on any of its equipment, network, or accounts. The Diocese may employ filtering technologies to limit access to sites on the Internet. If the Diocese discovers activities which do not comply with applicable law or Diocesan policy, records retrieved may be used to document the wrongful content in accordance with due process. The Diocese reserves the right to restrict or block non-business related Internet or network access at times of heavy network congestion in order to maintain essential business services.

It shall be the responsibility of the supervisor of a Diocesan employee to regularly monitor the use of the internet by his/her staff. Failure of a Diocesan employee to comply with any part of this policy, including inappropriate internet usage, may result in disciplinary action up to and including termination of employment.

ELECTRONIC SIGNATURES

Some Diocesan systems are equipped with electronic signature capabilities. The Diocese has certified to the FDA that electronic signatures are intended to be legally binding and equivalent to handwritten signatures. Therefore, anytime a Diocesan employee uses an electronic signature within a system, that signature is legally binding and equivalent to that employee's hand written signature.