Professional Standards and Rules of Conduct for Use of Information Resources
(Acceptable Use Policy)

PURPOSE AND SCOPE
The purpose of this policy is to establish the professional standards and business conduct related to the access and use of information and computer resources of the Archdiocese of Indianapolis. The policy applies to employees, contractors, volunteers, and officials.

DEFINITIONS
Users: Includes all employees, volunteers, contracted staff and consultants, and all other members of the Archdiocese to the extent they have authorized access to Archdiocesan information resources, and may include parishioners, volunteers, students, clergy, employees, contractors, consultants and volunteers.

Network Computing Environment: Servers, switches, network devices, connectivity, Internet resources, wireless resources, PCs, printers, scanners, and other electronic devices owned and operated by the Archdiocese.

Information Resources: A discrete body of information created, collected and stored in connection with the operation and management of the Archdiocese and used by Archdiocesan Network Users having authorized access as a primary source. Information Resources include electronic databases, electronic documents, images, videos, presentation materials, spreadsheets, and other electronic files.

GENERAL PROVISIONS
***Ownership and Monitoring**:* The Archdiocese provides Network Computing Environment access and Information Resources to users based on formal requests from management of the Secretariats and other operating units. These information resources and the resulting work products are the sole property of the Archdiocese of Indianapolis. The Information Resources and Network Computing Environment are to be used to the extent that they promote the mission of the Archdiocese, either directly or indirectly. While the Archdiocese does not typically monitor computer usage, the Archdiocese may on occasion monitor usage when an issue arises. There is no implied right to privacy for users of Archdiocesan Information Resources or Network Computing Environment.

Behavior Standards: All users of the Information Resources and Network Computing Environment are to adhere to high moral, legal, and professional standards, and are expected to support the mission and act in the best interests of the Archdiocese of Indianapolis. Users should not represent the Archdiocese in any official capacity using Archdiocesan Information Resources or the Network Computing Environment unless the user has been given explicit rights to do so by the Archdiocese.

Violations and Breaches: Users should report any security breaches or other abnormalities related to the Information Resources or Network Computing Environment of the Archdiocese to the Operational Support Center. Users should report any violations of this policy by other users to their Manager or to the Chief Information Officer. Non-compliance with these policies could result in disciplinary actions in accordance with Human Resources policies.

SPECIFIC STANDARDS AND RULES OF CONDUCT

All members of the Archdiocese community are to comply with the following policies, procedures, and security controls.

Network and Devices

1. Do not use the Network Computing Environment to gain unauthorized access to external networks.
2. Do not change the configuration of your PC, notebook or other computing device that has been provided to you by the Archdiocese, particularly virus protection, encryption, and other security software.
3. Always run Windows updates within a day of receiving notification to do so.
4. Only Archdiocese of Indianapolis provided IT equipment: desktop or laptop computer, tablets, smartphones, printers, scanners are permitted to connect to the corporate data network (wired or wireless). Personal devices are not permitted to connect to the corporate network unless approved by the CIO. Personal devices pose a risk of security vulnerabilities that could disrupt operation of the corporate network.
5. Do not attach unauthorized computing devices such as storage media, printers, and scanners to your PC or laptop or to the corporate data network.
6. Personal devices such as smart phones, tablets, laptops can be connected to the guest wireless network. The guest wireless network is password protected and password is available from the front desk or by contacting information system support center.
7. Personal device may be used to connect to your Archdiocese email. Before you do so, you must:
   - 7.1. Enable password protection on the device.
   - 7.2. Complete training information on mobile device security provided by the Archdiocese. To receive this training, contact the IT Support Center. Once training is complete email can be added on mobile device.

Internet Usage

1. During the onboarding process, you will be authorized by your manager for Internet usage and issued a personal user account (login id). Always access the Network Computing Environment using your authorized account.
2. All activities, communication, and electronic content must align with Archdiocesan behavior standards as outlined above or otherwise communicated by Human Resources.
3. Do not download or access unauthorized copyrighted, trademarked, or licensed software.
4. Do not download or access unauthorized copyrighted, trademarked, or licensed electronic information.
5. In order to conserve the resources of the Network Computing Environment such as bandwidth and storage capacity and protect information system security, do not play computer games, participate in online chat groups, participate in peer to peer file sharing, upload or download large files, stream audio and/or video files outside of the scope of your work.

Social Networking Sites

1. Use of social media (YouTube, Facebook, Twitter, Instagram, and Snapchat) should be limited unless it is pertinent to your job function. Access to these applications must be approved by your manager. Access to social network sites should be limited to personal devices which may connect to the guest wireless network.
2. If you are using a social networking account representing or “owned by” the Archdiocese on a social networking site, you must be authorized by your manager to do so. Contact your manager to obtain authorization.
3. When mentioning the Archdiocese in personal communications, appropriate behavior standards apply. See behavior standards above.
4. Do not use your Archdiocese email account as your account name to post personal or unauthorized messages to social networking sites.

Remote Access

1. Access to the Archdiocese network remotely using either a virtual private network interface or remote desktop capability must be authorized by your manager and by the Chief Information Officer. Contact your manager or Operational Support Center for authorization.
2. The same acceptable use standards, policies and procedures apply when using remote access.
3. Reasonable care must be used when transporting and using computing devices outside of the premises.
4. Information security standards and procedures must be followed (see section below) when using devices remotely.
5. Report lost computing equipment or lost personal devices with Archdiocese email account information to your Manager or the Operational Support Center immediately.

Security Access and Control

1. You must access information resources through your own assigned account. To obtain an account, see your manager.
2. When accessing software as a service or remote applications outside the network the same account and password standards apply whenever that is feasible based on the service provider capabilities.
3. Do not bypass standard access methods when using Information Resources.
4. Lock your computer (initiate "lock mode") if you will be away from your computer.
5. Passwords used to access the network and passwords used to access remote applications must be reasonably complex. The standards include:
   - 5.1. Must be at least 8 characters in length
   - 5.2. Must use at least one capital letter, one number, and one special character
   - 5.3. Must be changed every 90 days.
   - 5.4. Must be a new password, not a reused old password.
6. Do not set up shared accounts without authorization from your manager and the Chief Information Officer. See your manager for more information on authorizing shared accounts.
7. Do not use someone else's personal account or share passwords with other users.
8. Do not leave password information where it can be viewed by others.

Information Security (General)

1. Documents and other information resources should be stored in designated, secure network locations that are backed up by network-based backup and recovery systems. Documents and other information resources should not be stored on your PC or laptop unless required for your job. Circumstances such as making a presentation where you do not have access to the Internet to the Network Computing Environment may warrant storing a copy on your computer. In such instances, you should always have a copy of the document stored in an appropriate location.
2. The use of portable storage media should be limited. Portable storage media should always be scanned for viruses before use. Do not store protected information on these devices (see below).
3. Do not attempt to access data that you are not authorized to use or access.
4. On a quarterly basis, outdated information should be deleted from the Network Computing Environment and from your email account.

Information Security (Protected Information)

1. Special care is required for protected information. Protected information includes sensitive, confidential, health related (HIPPA), and personal information.
   - 1.1. Sensitive information includes information about the Archdiocese that might be controversial, under legal restrictions, or financially damaging to the Archdiocese.
   - 1.2. Personal information includes such items as social security numbers, checking account numbers, birth date, debit and credit card numbers.

1.3. Health related items include information such as prescription drug medications, mental or physical conditions.

1.4. Contact your manager or the Chief Information Officer for clarification on information that you suspect might fit into these categories.

2. Always store protected information where access is limited to authorized personnel.
3. Always encrypt protected information when it is stored or transmitted outside of the Network Computing Environment.
4. Share protected information only if required. Do not send unprotected sensitive or confidential information through normal email channels. Encrypted email capabilities are provided by the Archdiocese. Contact the Operational Support Center for instructions on the use of encrypted email.

Email

1. Never open an email from an unknown, suspicious, or untrustworthy source. If you open an email inadvertently, do not download any attachments or click on links or images in suspicious emails. Call the Operational Support Center if you are not sure about an email or if you think you may have an issue with a suspicious email.
2. Never download files from unknown or suspicious sources.
3. Do not auto-forward Archdiocesan emails to your personal email account unless required by your job and you have manager approval.
4. When setting up an Archdiocese email account on a personal device, see section labeled Network and Devices, item 7 for more information.
5. Do not accessing non-diocesan email accounts (Gmail, Yahoo Mail, etc.) on the Archdiocese. These accounts may not have spam filtering and pose a security risk. The guest wireless network can be used to access non-archdiocesan email using personal devices. Non-archdiocese email accounts please request approval from your manager.

Telephony

1. Your telephone is provided for business purposes. While use of your telephone is permitted for personal communications, that use should be limited as much as possible.
2. Your telephone should not be used to conduct private business related activities.
3. Do not incur long distance charges to the Archdiocese for personal phone calls.

Software and Applications

1. Do not sign up for or access “software as a service” applications (software residing on the Internet rather than on Archdiocesan network) without approval from your manager and the Chief Information Officer.
2. Use of storage and backup services (Dropbox, iCloud, etc.) should be limited unless approved as resources for Archdiocese use (Box.com). Use of these services may present a security risk to Archdiocese computers and servers. If there is a specific need for storage and backup services it must be approved by your manager and the Chief Information Officer. If access to files are needed when away from corporate network please request remote access through virtual private network or terminal services.
3. The use of freeware, screen savers, toolbars or other free software applications without approval is not permitted.
4. Do not download software without authorization from your manager and from the Chief Information Officer. Contact your manager or Operational Support Center for more information.

Notification Procedures

To report a problem or request additional information resources, contact the Operational Support Center. See the Intranet under Information Systems for information on how to contact the Operational Support Center.

Employer Name (printed): ____

Employer Name (signature): ____

Date: ______________________