ARCHDIOCESE OF
CINCINNATI
RADIATE CHRIST

INFORMATION TECHNOLOGY POLICY

INTRODUCTION

The Archdiocese and its Affiliates (defined as any entity that is subject to the administrative authority of the Archbishop of Cincinnati under Canon Law) use information technology and provide it to the employees of the Archdiocese. This policy sets forth the general rights and responsibilities common to all uses of information technology, from the stand-alone PC to the network systems in the Archdiocese/Affiliates.

This policy applies to all employees of the Archdiocese and its Affiliates, including guest users who have been given accounts on the Archdiocese's/Affiliates information technology systems for specific purposes. It also applies whether access is from the physical offices or from remote locations. In addition, there may be specific policies issued for individual systems, departments, and the like. While these principles must be consistent with this general policy, they provide more detailed guidance about what is permitted and prohibited on each system. All employees of the Archdiocese and its Affiliates are responsible for familiarizing themselves with any applicable policy prior to use. (See Records and Retention Policy for its related contents.)

GUIDING PRINCIPLES

The rights and responsibilities governing the behavior of employees of the Archdiocese and its Affiliates are the same on both the virtual and physical offices, and the same disciplinary procedures will be followed when the rules are violated. The user accounts, email accounts, computers and their contents are the property of the Archdiocese and its Affiliates**.** Any employee (including but not limited to lay personnel, priest, volunteer) that is assigned an email account must use that account for email communication for all Archdiocesan purposes. Section 3 of this document regarding Privacy provides additional information. **Computer users should have no reasonable expectation of privacy.**

SPECIFIC AREAS

1. Applicable Laws and Regulations

All employees of the Archdiocese and its Affiliates must obey:

- All relevant federal, state and local laws. These include laws of general application such as libel, copyright, trademark, privacy, obscenity and child pornography laws as well as laws that are specific to computers and communication systems, such as the Computer Fraud and Abuse Act and the Electronic Communications Privacy Act.

- All relevant Archdiocesan rules and regulations. These include the Rules of the Employee Policy Manual and all other Archdiocesan/Affiliate policies including the policy against sexual and racial harassment.
- The terms of all contracts and licenses applicable to the resources made available to users of information technology.
- This policy as well as other policies issued for specific systems.

2. Resource Limits

Information technology resources are often limited; what is used by one person may not be available to others. Many systems have specific limits on several kinds of resources, such as storage space or connect time. All users must comply with these limits and not attempt to circumvent them. Moreover, users are expected not to be wasteful of resources whether there are specific limits placed on them. Unreasonable use of resources may be curtailed.

3. Privacy

Employees of the Archdiocese and its Affiliates shall not attempt to access the private files of others. The ability to access a file does not, by itself, constitute authorization to do so.

The Archdiocese and its Affiliates do not routinely monitor or inspect individual accounts, files, or communications but reserve the right to do so when necessary, including but not limited to: (1) system managers may access user accounts, files or communications when there is reason to believe that the user is interfering with the performance of a system; (2) authorized investigators may access accounts, files, or communications to obtain relevant information when there is a reasonable suspicion that the user has violated either laws or Archdiocesan policies; (3) co-workers and supervisors may need to access accounts, files, or communications used for Archdiocese/Affiliate business when an employee becomes unavailable; and (4) when required by law. All monitoring and inspection shall be subject to authorization, notification and other requirements specified in the Use of Information Technology Policy.

Though the Archdiocese and its Affiliates will attempt to prevent unauthorized access to private files, it cannot make any guarantees. Information also can be revealed by malfunctions of computer systems, by malicious actions of hackers, and by deliberate publication by individuals with legitimate access to the information. Users are urged to use caution in the storage of any sensitive information. **Again, users should have no reasonable expectation of privacy.**

4. Access

Some portions of the Archdiocesan/Affiliate Network, such as public web pages, are open to everyone. Other portions are restricted in access to specific groups of people. No one is permitted to enter restricted areas without authorization or to allow others to access areas for which they are not authorized. The ability to access a restricted area does not, by itself, constitute authorization to do so. Individual accounts are for the use of the individual only; no one may share individual accounts with anyone else, including members of the account holder's family. Joint access to resources should be provided from separate accounts.

5. Security

All employees of the Archdiocese and its Affiliates must assist in maintaining the security of information technology resources. This includes physical security, protecting information and preventing and detecting security breaches. Backup computer data and information that is out of the scope of the Pastoral Center's backup and disaster recovery procedures would require that computer information containing Personal Identifiable Information must be kept in fireproof storage and under lock and key. In order to limit misuse or theft of Personal Identifiable Information, employees are never allowed to take this information off Archdiocesan/Affiliate premises. Passwords are the keys to the Archdiocesan/Affiliate computer system and all users are responsible for the security of their passwords. Users must report all attempts to breach the security of computer systems or networks to the Department Director or the Manager of Information Systems.

Backup

- **Archdiocesan Pastoral Center**
  Data backup and disaster recovery solutions will be reviewed annually. Data backup is to begin as a seed backup (Full backup). Daily incremental backups continue for a 30-day window. After 30 days all backups are expired except for the last full backup of files currently on the servers. Monthly off-site full backups are created and retained for a 90 day retention period. Recovery of data is guaranteed within two (2) business days of request for restore. Every attempt to backup data in its entirety will be made. However, usage of data files during the backup process, mechanical failure, power and environmental conditions may limit the quantity and quality of backup data. (For details of emergency or disaster recovery, see language in contract.)

- **Stewardship**
  Stewardship donor and donation data is backed up weekly via scheduled archive file within the Stewardship office's Salesforce account, by Stewardship staff, then moved into the Archdiocesan Microsoft SharePoint cloud storage and held for six months.

- **EthicsPoint**
  EthicsPoint backups are run on a nightly basis and are stored in an off-site facility through encrypted and secure channels. Backend database servers are operated in a clustered environment with a creative-passive configuration. Backups are available at all times if there were ever a need to restore data. EthicsPoint servers are stored in a locked physical environment that includes 24x7 security guards. All communication between the EthicsPoint site and user's web browser are accomplished using 128-bit SSL encryption and Verisign® certificates to protect confidential data. (For details of emergency or disaster recovery, see language in contract.)

- **Paylocity**
  Paylocity backups conform to industry accepted standards in accordance with the AICPA's Statement on Standards for Attestation Engagements No. 18 (SSAE 18) with the SOC 1 Type 2 and SOC 2 Type 2 report results from Crowe LLP's test procedures available for review from the Director of Information Systems.
- **Affiliates**
  Archdiocese of Cincinnati Affiliates are responsible for backing up their systems.

- **Antivirus/Malware**
  Every effort is made by administrator(s) of the network to keep current antivirus software on our network and its computers. All files are configured to be scanned for viruses and malware, in real-time from all incoming sources (i.e. CD-ROM, Floppy Diskette, Email Attachment). User accounts are configured to reduce the risk of downloading and/or installing software before it has been evaluated by an administrator. No attempt to circumvent this configuration by a user should be made. All users are expected to notify an administrator if they feel a virus or malicious software has infected their computer

6. Plagiarism and Copyright

Intellectual honesty is of vital importance in the Archdiocese and its Affiliates. You must not represent the work of others as your own. You must respect the intellectual rights of others and not violate their copyright or trademark rights. It is especially important that you obey the restrictions on using software or library resources for which the Archdiocese has obtained restricted licenses to make them available to employees of the Archdiocese and its Affiliates.

7. Enforcement

Anyone who becomes aware of a possible violation of this policy or the more specific regulations of the systems that comprise the computer system should notify the relevant Department Director or System Administrator. The System Administrator will investigate the incident and determine whether further action is warranted. The System Administrator may resolve minor issues by obtaining the agreement that the inappropriate action will not be repeated. In those cases that warrant disciplinary action, the System Administrator will refer the matter to the Human Resources Director.

The System Administrator can act to block access and disable accounts when necessary to protect the system or prevent prohibited activities, but such actions cannot be used as punishments. Users must be notified promptly of the action and the restrictions must be removed unless the case is referred for disciplinary action.