Policy Title: Information Technology Systems

Effective Date: January 1, 2009
No. of Pages: 7 & Employee Acceptance Page

Diocese of Springfield in Illinois

Section I *– General Statement*

1. Information Technology Systems (ITS), when properly used, provide timely communication and technological support to help fulfill the mission of the Church. This policy contains principles and practices designed to ensure that Information Technology Systems are used in ways that are consistent with the mission and that will avoid use of the systems for, illegal, immoral, or unethical purposes. The Bishop of the Diocese of Springfield in Illinois reserves the right to amend or revise this document, in whole or part, at any time. Written notification of the change will be provided by the Bishop or the Vicar General Moderator of the Curia.

Section II *-- Policy Application*

2. This policy applies to all priests and deacons incardinated in the Diocese of Springfield in Illinois, other priests and deacons who have the faculties of the Diocese of Springfield in Illinois, seminarians of the diocese, members of institutes of consecrated life and societies of apostolic life (religious) and lay persons who are employed full-time or part-time, in the parishes, schools, agencies and other institutions of the Diocese of Springfield in Illinois, and all persons who as volunteers use diocesan supplied ITS or are guest users as described in this policy.

Section III *- Definitions*

3. *Information Technology Systems* include, but are not limited to, computers, computer networks, PDAs (personal digital assistants), fax machines, telephones (land lines and mobile), voice mail, audio and video teleconferencing devices, video equipment, software, operating systems, storage media, network accounts providing electronic mail, handheld devices, photocopying machines, printers, and typewriters owned by the Diocese, its parishes, agencies, or institutions.

4. *Diocese* as used in this policy refers to the parishes, parish schools, diocesan sponsored schools, the curia, commissions, councils, committees, task forces, boards, advisory boards, agencies and institutions sponsored by the Diocese of Springfield in Illinois.

5. *Users* of ITS are the persons described above under “Policy Application” of the diocese of Springfield in Illinois.

6. *Guest Users* of the ITS are *system administrators* who are outside consultants or contracted by the *Administrative Authority*, vendors, technicians or other persons who are allowed to access ITS, but are not employed by the *Diocese.*

7. *Administrative Authority* is a *User* with the authority to authorize access to staff, volunteers, and *Guest Users* to access data in accordance with the ITS Policy. The following list further defines the *Administrative Authority*:

Curia	Vicar-General/Moderator of the Curia
Parish	Pastor, Administrator, Priest Moderator, Parish Life Coordinator
Parish School	Principal
Diocesan sponsored school	Principal
Catholic Charities	Executive Director

The Bishop of the Diocese of Springfield in Illinois may act, as need arises, as the *Administrative Authority* for the curia or any parish, parish school, diocesan sponsored school, commission, council, committee, task force, board, advisory board, agency or institution sponsored by the Diocese of Springfield in Illinois.

The Administrative Authority is the only individual who may authorize compliance checks. If the Administrative Authority listed above is suspected of misusing the system, the Bishop will act as the Administrative Authority or appoint an alternative Administrative Authority over the impacted parish, parish school, diocesan sponsored school, the curia, commissions, councils, committees, task forces, boards, advisory boards, agencies and institutions sponsored by the Diocese of Springfield in Illinois.

8. *System Administrator* is a *User* responsible for monitoring the functioning of the ITS for a particular parish, parish school, diocesan sponsored school, the curia, commission, council, committee, task force, board, advisory board, agency or institution sponsored by the Diocese of Springfield in Illinois. The system administrator is appointed by the head of the parish, parish school, diocesan sponsored school, the curia, commission, council, committee, task force, board, advisory board, agency or institution sponsored by the Diocese of Springfield in Illinois.

9. *Guest System Administrator* is a *Guest User* that is an outside consultant or contractor entrusted with the responsibility for monitoring the functions of the IT system.

10. *Directives* are the policies and guidelines issued by a particular parish, parish school, diocesan sponsored school, commission, council, committee, task force, board, advisory board, agency or institution sponsored by the Diocese of Springfield in Illinois.

Section IV *-- General Policy applying to parishes, parish schools, diocesan sponsored schools, the curia, commissions, councils, committees, task forces, boards, advisory boards, agencies and institutions sponsored by the Diocese of Springfield in Illinois.*

Article 1 - General Provisions

11. Information Technology Systems and equipment purchased or provided by the Diocese and related agencies, schools, and institutions, and all information, messages and files created with the aid of the ITS in the performance of Diocesan ministry and business are the property of the Diocese and are subject to reasonable inspection as outlined in this policy.

12. Parishes, parish schools, diocesan sponsored schools, the curia, commissions, councils, committees, task forces, boards, advisory boards, agencies and institutions sponsored by the Diocese of Springfield in Illinois may develop *Directives* particular to its mission and operation. Such *Directives* must be consistent with the ITS Policy.

13. *Users* who violate the policy may face suspension of ITS privileges and/or other disciplinary action up to and including reassignment, termination of employment or volunteer position, and other discipline as deemed appropriate.

Article II- Acceptable Use

14. Information Technology Systems are to be used for business and ministerial purposes. The Diocese allows minimal, occasional or incidental personal use of ITS (sending or receiving) for non-business purposes. Personal use must not in anyway interfere with or impede the Diocese's mission, must be occasional and minor, must be promptly discontinued at the request of the *Administrative Authority*, and is expressly subject to all of the provisions of this policy.

15. Users who use ITS for personal communications without express permission are subject to bearing the cost of their unauthorized use.

16. Priests and seminarians residing in parish or diocesan owned housing may use ITS for personal communication as long as such use does not violate other provisions of this policy. Personal literary creations authored by a priest, deacon, or seminarian made with the aid of ITS belong to priest, deacon, or seminarian. All communication on ITS, however, are subject to monitoring by the Administrative Authority.

Article III - Unacceptable Use

17. Creating or issuing personal communications that appear to be an official communication of the Diocese without proper authorization.

18. Using ITS in such a way that it interferes with the employee's productivity or creates unnecessary expense or violates the *Directives* of a parish, parish school, diocesan sponsored school, the curia, commission, council, committee, task force, advisory board, agency or institution sponsored by the Diocese of Springfield in Illinois.

19. Disseminating or intentionally accessing material that is in the sole discretion of the Administrative Authority considered defamatory, abusive, obscene, profane, sexually suggestive, pornographic, harassing, intimidating, threatening, racially offensive, illegal, gambling related, fraudulent, or otherwise inappropriate or illegal written, recorded, or electronically retrieved or transmitted communication; nor shall the user encourage the use, sale or distribution of controlled substances or other illegal activity. The Administrative Authority may exempt those persons whose ministry or job may necessitate access to such material, including when a *System Administrator* conducts a compliance check.

20. Disseminating the Diocese's confidential information to persons, organizations or agencies, including other entities sponsored by the Diocese, unless authorized by the *Administrative Authority*. Confidential information includes all information that is not generally available to the public, including but not limited to, financial information, personnel files, personal information provided by members of the church, or any information deemed confidential.

21. Hacking or attempting to gain illegal or unauthorized access to secured or restricted sites.

22. Deliberately damaging or tampering with computers or other ITS components.

23. Violating copyright laws, including the acquisition, use or distribution of pirated software.

24. Downloading proprietary materials or information (e.g., customer lists, product information, databases, etc., trademark or patented materials, copy write music) without the owner's permission.

25. Using someone else's Username or password (except as provided under Required Best Practices).

26. Trespassing in another *User's* folder, files, or work, unless searching in another Users' folder, files or work is authorized by an Administrative Authority for purposes of obtaining information needed to conduct the business of the parish, parish school, diocesan sponsored school, the curia, commission, council, committee, task force, board, advisory board, agency or institution sponsored by the Diocese of Springfield in Illinois or for monitoring or inspection purposes.

27. Using the ITS for commercial purposes, private financial or commercial gains, commercial or private advertising, product advertisement nor for the establishment of personal web pages. Unauthorized "chat" or chain letter communication is also prohibited.

28. Intentionally introducing a virus, worm, Trojan horse or other code that will disrupt ITS.

29. Changing ITS settings unless authorized by an ITS *System Administrator*.

30. Installing software or hardware unless authorized by the ITS *System Administrator*.

31. Downloading entertainment software or games, or playing computer games against opponents over the Internet.

32. Downloading images or videos unless there is an explicit business-related use for the material.

33. Making political lobbying or making political or social announcements not directly connected with the Diocese.

34. Removing ITS equipment from the premises without the express written permission of the *Administrative Authority*. Equipment designated for check out (e.g. multi-media projectors, laptop computers) is exempted.

35. Removal of printed paper-based confidential information from the premises of any diocesan entity is not allowed without the authorization of the Administrative Authority. Confidential information in electronic format can be removed from the premises provided the documents are stored in a diocesan approved secure USB storage unit that encrypts the data to protect it against loss and potential unauthorized use. The diocesan Associate Director of IT can provide these storage units with training upon request.

36. Storage of Electronic Files. It is not acceptable to store files of the diocese or related parishes, parish schools, agencies, and institutions on any non-diocesan owned computer or other storage device at any time. The only acceptable method of storing for use with equipment not owned by the parish, parish school, school, diocesan sponsored school, the curia, commission, council, committee, task force, board, advisory board or institution sponsored by the Diocese of Springfield in Illinois is the secure USB storage unit that is available from the diocesan Associate Director of IT upon request.

37. Using personal email accounts to send or receive information related to the business of the diocese, related parishes, parish schools, agencies, and institutions, or accessing personal email accounts for personal reasons while on the job is not permitted.

38. Using ITS equipment or systems in a manner that would result in violations of other diocesan policies.

Article IV - Access and Privacy

39. Electronic communications to include email messages should be crafted with care and the understanding that all such communications are subject to monitoring by the Administrative Authority, could be subject to monitoring by outside agencies, and maybe subject to third-party legal disclosure and subpoena.

40. *User*s must maintain the secrecy of their passwords. Emergency access procedures are described under Required Best Practices. It is, however, understood that the purpose of passwords is for network security and not for the personal privacy of a user.

41. The *Administrative Authority* may authorize access to any and all files stored in private areas of the network and hard drives, discs, and other storage devices in order to assure compliance with the policy and *Directives*.

    a. The *Administrative Authority* may authorize an outside consultant or contractor to access components of the ITS if such access is necessary for the consultant or contractor to perform a service for the diocese. These *Guest Users* or *Guest System Administrators* are expected to comply with the provisions of Article IV of this policy when using ITS components owned by the Diocese.

b. The *System Administrator* employed by the *Administrative Authority* may authorize an outside technician or consultant to access ITS for the purposes of maintenance, repair, or evaluation with the authorization of the Administrative Authority.

Article V - Compliance

42. The *Administrative Authority* may authorize random compliance audits which may include access to any component of ITS at any time, with our without notice to the *User*.

Section V *-- Best Practices*

Article I - General Provision

43. The *Administrative Authority* is free to develop or oversee the development of Best Practices specific to the parish, parish school, diocesan sponsored school, the curia, commission, council, committee, task force, advisory board, agency or institution sponsored by the Diocese of Springfield in Illinois for which the *Administrative Authority* is responsible.

Article II - Required Best Practices

44. Install Antivirus software. The diocesan Associate Director for Information Technology can provide effective low cost software.

45. Install a firewall for networks.

46. Implement a data and equipment back-up, retention and destruction plan that provides for an orderly, cost effective, and secure back-up, storage and eventual destruction plan for all data and equipment. Contact the diocesan Associate Director for Information Technology for consultation to set up a plan.

47. To provide emergency access to accounts each *User* should write out his or her user name and password, place it in a sealed envelope and place the envelope in a secure place where the *Administrative Authority* can access it if necessary. Emergencies include the death or incapacitation of the *User.*

48. Users using a personally-owned home computer for job related purposes must meet diocesan minimum security standards including current anti-virus and anti-malware protection. The diocesan Associate Director for Information Technology (IT) can provide effective low cost software that can be installed to meet these minimum standards. Certification of this minimum standard must be obtained from the Associate Director for IT prior to using a personally-owned home computer to access Information Technology Systems of the diocese, related agencies, parish, school or other institution.

Article III - Recommendations for Best Practice

49. The *Administrative Authority* is urged to implement Recommendations for Best Practice to the degree that the Recommendations address the needs of each parish, parish school, diocesan sponsored school, the curia, commission, council, committee, task force, advisory board, agency or institution sponsored by the Diocese of Springfield in Illinois.

50. Use care in creating email messages as the contents are neither private nor confidential. Even when a message has been deleted it may still exist on a back-up system, be restored, be printed out, or may have been forwarded to someone else without the creator's knowledge. Email messages may be subject to third-party legal disclosure.

51. Do not install personally owned hardware or software without the authorization of the *System Administrator or the Guest System Administrator*.

52. The *Administrative Authority* should develop a job description for the *System Administrator*. If serving as *System Administrator* is not the primary job function of the individual or the individual is a *Guest System Administrator* develop a task list relating to the responsibilities required to be performed for ITS.

53. Refrain from downloading or sending unsolicited advertisements, cute stories, cute pictures, jokes, free screensavers and desktop backgrounds, emotion icons and other "Free" products; they often contain spy ware or viruses.

54. Do not allow guests, including children, to use an office computer or other ITS device as entertainment. System security could be compromised.

Article IV - Useful Information

55. For virus information consult http://www.sarc.com

Policy Acknowledgement

By signing this document I acknowledge having received a copy of, and I hereby confirm that I have read and have agreed to comply with the terms of the Information Technology Systems Policy of the Diocese of Springfield in Illinois.

_____ Date_____
Signature