INFORMATION TECHNOLOGY

SYSTEMS POLICY

OF THE ARCHDIOCESE OF MALTA

IT Services – Archdiocese of Malta

Policy Title: *Information Technology Systems*
Effective Date: *25th August 2015*
Archdiocese of Malta

Section I – General Statement

1. Information Technology Systems (ITS), when properly used, provide timely communication and technological support to help fulfil 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. This policy has to be taken in conjunction with the E-mail and internet acceptable use policy. The Archbishop of the Archdiocese of Malta 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 Archbishop or the Vicar General or their delegate.

Section II -- Policy Application

2. This policy applies to all priests and deacons incardinated in the Archdiocese of Malta, other priests and deacons who have the faculties of the Archdiocese of Malta, seminarians of the Archdiocese, members of institutes of consecrated life and societies of apostolic life (religious) and lay persons who are employed full-time or part-time, at the Archbishop's Curia, Ecclesiastical Tribunals, parishes, schools, entities and other institutions of the Archdiocese of Malta, 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), mobile devices including tablets, 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, entities, or institutions.

4. Diocese as used in this policy refers to the parishes, parish schools, Church Schools, the Curia, commissions, councils, committees, task forces, boards, advisory boards, entities and institutions sponsored by the Archdiocese of Malta.

5. Users of ITS are the persons described above under "Policy Application" of the Archdiocese of Malta.

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 Archdiocese of Malta.

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:

Vicar-General

Administrative Secretary

Archbishop's Delegates

Director of IT Services

Parish Priest, Administrator, Rector,

Church School Principal

Entities Director/Administrator

The Archbishop of the Archdiocese of Malta may act, as need arises, as the Administrative Authority for the curia or any parish, church school, commission, council, committee, task force, board, advisory board, entity or institution sponsored by the Archdiocese of Malta.

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 Archbishop will act as the Administrative Authority or appoint an alternative Administrative Authority over the impacted parish, school, the curia, commissions, councils, committees, task forces, boards, advisory boards, entities and institutions sponsored by the Archdiocese of Malta.

8. System Administrator is a User responsible for monitoring the functioning of the ITS for a particular parish, Church School, the Curia, commission, council, committee, task force, board, advisory board, entity or institution sponsored by the Archdiocese of Malta. The system administrator is appointed by the Parish Priest, Church School, the Curia, commission, council, committee, task force, board, advisory board, entity or institution sponsored by the Archdiocese of Malta.

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, Church School, commission, council, committee, task force, board, advisory board, entity or institution sponsored by the Archdiocese of Malta.

Section IV -- General Policy applying to parishes, Church Schools, the Curia, commissions, councils, committees, task forces, boards, advisory boards, entities and institutions sponsored by the Archdiocese of Malta.

Article 1 - General Provisions

11. Information Technology Systems and equipment purchased or provided by the Diocese and related entities, 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. Parish, Church School, the Curia, commission, council, committee, task force, board, advisory board, entity or institution sponsored by the Archdiocese of Malta 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, Church School, the Curia, commission, council, committee, task force, board, advisory board, entity or institution sponsored by the Archdiocese of Malta.

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, Church School, the Curia, commission, council, committee, task force, board, advisory board, entity or institution sponsored by the Archdiocese of Malta 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, netbooks, tablets) 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.

36. Storage of Electronic Files. It is not acceptable to store files of the diocese or related parishes, church schools, entities, 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, Church School, the Curia, commission, council, committee, task force, board, advisory board, entity or institution sponsored by the Archdiocese of Malta is a secure USB storage unit.

37. Using personal email accounts to send or receive information related to the business of the diocese, related parishes, Church schools, entities, and institutions is not permitted.

38. Using ITS equipment or systems in a manner that would result in violations of other diocesan policies is not permitted.

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. Users 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.

- 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.

- 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 or 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, Church School, the Curia, commission, council, committee, task force, board, advisory board, entity or institution sponsored by the Archdiocese of Malta for which the Administrative Authority is responsible.

Article II - Required Best Practices

44. Install Antivirus 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 Archdiocesan IT Team 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. Certification of this minimum standard must be obtained from the IT Team prior to using a personally-owned home computer to access Information Technology Systems of the Archdiocese, related entities, 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, Church School, the Curia, commission, council, committee, task force, board, advisory board, entity or institution sponsored by the Archdiocese of Malta.

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 IT Team or the Guest System Administrator.

52. 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.

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

Article IV - 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 Archdiocese of Malta.

_____ _____

Signature *Date*