EPISCOPAL CONFERENCE OF MALAWI

Information and Communications Technology – ICT Policy

Catholic Secretariat

P.O. Box 30384

LILONGWE 3

Telephone: +265 1 772 204

Email: ecm@ecmmw.org

Website: www.ecmmw.org

An ICT-led ECM

May 2019

TABLE OF CONTENTS **Page**

LIST OF ACRONYMS ABBREVIATIONS

AMECEA:	Association of Member Episcopal Conferences of Eastern Africa
ECM:	Episcopal Conference of Malawi
ICT:	Information and Communication Technology
IPC:	Internal Procurement Committee
MACRA:	Malawi Communications Regulatory Authority
NICTP:	National Information and Communications Technology Policy
PDA:	Personal Digital Assistant
SG:	Secretary General
SRCC:	Social Research and Communication Commission
UPS:	Uninterrupted Power Supply

FOREWORD

The Episcopal Conference of Malawi (ECM) is the national organization of the local Catholic hierarchy, constituted with the approval of the Holy See and registered in accordance with the Laws of Malawi, by which jointly exercises its pastoral office to promote common good of the people of God entrusted to its care particularly by deliberating on matters of common interest and enacting forms and methods of the Apostolate adapted to the existing circumstances. Currently, ECM is an assembly of eight dioceses which are: Blantyre, Chikwawa, Dedza, Karonga, Lilongwe, Mangochi, Mzuzu and Zomba.

ECM is committed to providing well-coordinated holistic Evangelisation through teaching the Word of God, Sacraments and facilitating integral human development. ECM strives to promote coordination and networking in order to ensure sharing of information and resources, to avoid duplication and competition for resources among commissions, departments and directorates.

In this regard, the Catholic Bishops of the ECM are happy to approve and present to you this Information and Communication Technology – (ICT)policy which will guide the aspirations and operations of the entire Catholic Church in Malawi under the Episcopal Conference of Malawi (ECM for the next three years (2019-2021).

ECM ICT policy comes as a response to the 18thAssociation of Member Episcopal Conferences of Eastern Africa (AMECEA) Plenary held in Lilongwe, Malawi in July 2014. During the plenary, Bishops were challenged to harness the use of and the negative influence of ICT and social media in the evangelization work of the Church. It was since resolved that an ICT Policy should be enacted both at regional and national level.

This Policy document serves as a moral compus in the use of ICT and social media in the Church while upholding the Christian virtues that underpin the ECM values.

Most Rev. Thomas Luke Msusa

CHAIRMAN, EPISCOPAL CONFERENCE OF MALAWI

PREFACE

The approach and methodology used in the development of this ICT policy has been participatory and consultative. Various stakeholders made valuable contributions during the national and diocesan consultative meetings brought together all concerned communication stakeholders from all the Archdioceses and Dioceses.

I believe, therefore, that the responsibility for the effective and successful implementation of this ICT policy depends on the strengths of all concerned communication stakeholders, the Catholic Church members and Church groups, Commissions, departments and directorates.

I want to take this opportunity to thank the Bishops' Conference for entrusting me and the Catholic Secretariat's Communication Commission with this very important task. I wish also to thank all those who participated in the consultative meetings for their valuable commitment, input and love.

I want to thank all partner organizations for their financial and material support during the development of this ICT Policy.

Rev. Fr. Henry Saindi

SECRETARY GENERAL

1.0) ECM VISION, MISSION AND CORE VALUES

The strategic framework will be guided by the following vision, mission and core values which the Catholic Church in Malawi wishes to achieve in the next five years.

1.1) VISION

Family of God filled with the Holy Spirit living in love.

1.2) MISSION

The Catholic Church in Malawi is committed to providing well-coordinated holistic Evangelisation through teaching the Word of God, Sacraments and facilitating integral human development.

1.3) CORE VALUES

The implementation of this strategic framework is guided by the following core values and beliefs:

1.3.1) Love

"Love one another as I have loved you" (John 15:12). Love is the core value of the Christian life. As missionary disciples of Jesus Christ, all Catholic members are invited to live the love of God in the family, Small Christian Community, Church and society.

1.3.2) The Dignity of the Human Person and Sanctity of Life

The dignity of the human person is a fundamental value. This is based on the fact that the human being is God's creation. "So God created mankind in his own image, in the image of God he created them; male and female he created them" (Gen. 1:27). This dignity of every human being is what is at the foundation of human rights and corresponding responsibilities.

1.3.3) Common Good

The Common Good is understood as a value coming from all necessary conditions of social living – economic, political, material, religious, cultural - which enable men and women to more readily and more fully realize their human dignity and achieve their full human potential. The promotion of the common good should be the concern of the Church.

1.3.4) Solidarity

The principle of solidarity comes from the very notion of society in its commitment to the common good. We belong to one human family and as such have mutual obligations to promote the development of all people across the world.

1.3.5) Principle of Subsidiarity

Social institutions must leave to the smaller groupings or individuals what they can do by their own power; on the other hand, they must assist the smaller groupings or individuals where they are unable to accomplish a necessary task. This means a higher level of the Church should not perform any function or duty that can be handled more effectively at a lower level by people who are closer to the problem and have a better understanding of the issue.

1.3.6) Preferential Option for the Poor

A preferential option for the poor is a commitment by Catholic members and the community at every level to engage actively in a struggle to overcome the social injustices which affect our world. "Poor" is understood to refer to the economically disadvantaged who, as a consequence of their status, suffer oppression and powerlessness. Such solidarity also means a commitment to working with structures, organizations and agencies that promote the interests of the less privileged in society i.e. the economically poor, the groups that are politically marginalized and people discriminated against. Therefore, in every economic, political and social decision, a weighted concern must be given to the needs of the poorest and most vulnerable.

1.3.7) Stewardship and integrity of creation

Our commitment to the common good requires responsible stewardship of the earth and its resources. True stewardship calls us to examine how we use and share the goods of the earth, what we pass on to future generations, and how we live in harmony with God’s creation. By our work, we are co-creators in the continuing development of the earth. This core value will be guided by Papal document on Care for Environment, *Laudato Si*.

1.3.8) Justice and Peace

Society ensures social justice by providing the conditions that allow associations and individuals to obtain their due. The equal dignity of human

persons requires the effort to reduce excessive social and economic inequalities. To promote justice is to transform structures which block love. The concern for justice is not an option but a constitutive part of evangelization. Thus, action on behalf of justice and participation in the transformation of the world fully appear to us as a constitutive dimension of the preaching of the Gospel. Peace is the fruit of justice and is dependent upon right order among human beings and among nations.

1.3.9) Moral integrity and accountability

This is a commitment to being transparent, accountable, honest, trustworthy, and of moral integrity in all activities. This entails protecting the interests of our Church and to maintaining its integrity in carrying out pastoral duties and programs. This may demand carrying out our duties in an efficient, effective and non-discriminatory manner.

2.0) WHY HAVE AN ICT POLICY?

Every organization needs to inform its people about the type of behaviour it expects of those using technology in the workplace and about the consequences for abusing technology privileges. It is a good practice and often a requirement to conform to quality standards in ICT.

Policies exist for the security, protection, user safety, good practice and guidance for an organisation. It also gives individual users ground rules for acceptable use of ICT equipment so that there are no misunderstandings. This document will also provide a guideline to deal with misuse of equipment or information. At the same time, it demonstrates that ECM is professional in its approach to managing ICT users and resources.

3.0) OBJECTIVES AND SCOPE

3.1) Objectives

All ICT infrastructure and facilities remain the property of ECM and the purpose of this policy is to ensure acceptable and appropriate care and use. The objectives of this ECM policy therefore are to:

a) Ensure efficient and effective use of information systems by ECM personnel;
b) Enhance information and technology security within ECM;
c) Minimize the risk of systems failures;
d) Guide availability of ICT systems; and
e) Ensure compliance with Malawi's relevant legislations and policies such as National ICT Policy and Guidelines as provided by regulator in the field of ICT – the Malawi Communications Regulatory Authority (MACRA).

3.2) Scope

This ICT policy relates to all information technology facilities and services provided by ECM including email communications, databases, internet, telephones systems, printers, facsimiles and photocopiers. All the ICT infrastructure and facilities are intended for use in the best interest of ECM. It is therefore imperative to observe proper use and care of such facilities.

As and when need arises, it may be necessary to amend and formulate an operational manual for certain aspects of this policy.

4.0) Policy details

4.1) General user and ownership

4.1.1) All users of ICT facilities within ECM should remember that any data they create or generate on the systems remains the property of ECM.

4.1.2) All personnel are responsible for exercising prudence in personal use of ICT facilities of ECM, particularly in respect of impact on one's performance of official work and cost to ECM.

4.2) Security and proprietary information

4.2.1) It is the responsibility of each authorized ECM personnel to ensure proper security for their respective passwords, accounts and any assigned ICT equipment.

4.2.2) It is imperative that all ECM institutional data is protected in a manner that is considered reasonable and appropriate in terms of value, sensitivity and critical nature to ECM's work and mission.

4.2.3) It is important for all ICT users to exercise special care of information on portable computers such as laptops as such information is vulnerable.

4.2.4) Users of ECM email systems should exercise due care when opening email attachments received from unknown senders to avoid exposure to viruses, email bombs or Trojan horse codes.

4.3 Network systems

4.3.1) ECM shall install across its entire network, effective firewalls and intrusion detection systems to monitor and prevent hackers, viruses and worms.

4.3.2) All computers linked into ECM's network shall have an up-to-date anti-virus software to prevent viruses and all other forms of malicious attacks. Similarly, extreme care should be exercised before hooking any laptop to the network.

4.3.3) Software that requires a license must not be installed until the license is duly obtained by the Manager responsible for ICT. It is illegal to circumvent license procedures.

4.3.4) Care should be exercised to avoid copying files onto one's personal directory that are centrally accessible unless there is a justifiable reason.

4.3.5) ECM will put in place a suitable back up strategy so that all valuable data and software can be recovered.

4.3.6) Live streaming and downloads of movies and pornographic videos must be prohibited.

4.4. Email and communications. (CF Appendix 1Communication Strategy)

Communication by electronic mail (email) has proved very popular both within ECM and with external persons or institutions. The email function is to support ECM's mission. Notwithstanding the fact that users may use email for personal issues, it therefore becomes imperative to observe certain basic guidelines as follows.

4.4.1) All emails sent or received by ECM will be subject to automatic virus scanning by the central ECM email gateway.

4.4.2) As an ICT user of ECM equipment, and as long as the ECM official email address is used, each staff is a representative of ECM

and therefore it is important to ensure that all one's actions are in the interest of ECM and avoid exposing ECM to legal suit on account of what is published in one's email.

4.4.3) Staff should use ECM email for only official communication. It is not advisable to use a webmail account such as Gmail, Hotmail or Yahoo or even a personal email account when the email contains ECM work related information or communication.

4.4.4) Use of email is often in preference to paper to reach addressees quickly and to reduce on use of paper, but it is cardinal to think and check messages before sending to ensure that it is well phrased and sent to the correct addressee.

4.4.5) It is important to send an email only to the person or to persons it is meant for, rather than distributing to unnecessary persons as this has the effect of affecting computer and network performance and wastes disk space.

4.4.6) Similarly, it is not advisable to broadcast emails with attachments to a large group of people because it puts unnecessary load on the network.

4.4.7) Electronic files should hold electronic correspondence that has to be kept, but should not be printed and kept on paper files unless it is absolutely necessary.

4.4.8) It is advisable to keep one subject per email when the content is complex as this simplifies filing and retrieval later.

4.4.9) ICT users of ECM and members of staff should not allow anyone to send emails using their email address. Email users are responsible for the content of all emails sent in their name and from their address.

4.4.10) ICT users of ECM should not forward internal email with sensitive content to personal email address on external networks such as Gmail, Hotmail etc.

4.4.11) All warnings of virus attacks that do not originate from an authorized source should be reported to the manager or administrator responsible for ICT. It is not necessary to send such warnings to friends or other persons as though the message is authentic, with the person sending such message or ECM as the originators.

4.4.12) All ICT users of ECM should not open email unless one has reasonably good expectation of what the email contains and the source of the said email.

4.5 Health and safety

It is cardinal to observe the working environment to avoid conditions that might adversely affect the operation of the ICT equipment. Emergency and alarm systems should be tested regularly. The manager/administrator responsible for the ICT portfolio should therefore ensure regular monitoring for the state of the following:

4.5.1) Electrical power supply, inclusive of trailing cables or leads that could constitute a health hazard and excessive loading on the extension sockets.
4.5.2) Possible water leakage.
4.5.3) Fire and smoke detection and control.
4.5.4) Air condition in terms of correct level of humidity and temperature.
4.5.5) Uninterrupted Power Supply (UPS) installations.
4.5.6) Damaged chairs and other hazardous equipment.
4.5.7) Computer settings i.e. brightness and contrasts of monitors.

ECM will ensure that all unsatisfactory working environments are identified and rectified.

4.6 Software

4.6.1) The manager/administrator under whom the ICT portfolio falls is responsible for ensuring timely updating of anti-virus software. It is also incumbent upon any ICT user to make a timely report to the responsible manager/administrator on any outdated versions of anti-virus for action.

4.6.2) The manager/administrator is also responsible for keeping, on behalf of ECM, licenses of various software.

4.6.3) The manager/administrator in charge of ICT within ECM shall ensure that new software is purchased only after careful evaluation and fits the purpose for which it is intended for ECM use.

4.6.4) Under no circumstances is any ICT user within ECM permitted to use software from external sources.

4.6.5) Installation of software on the server or local machine shall be done by ICT office or upon permission from ICT office.

4.6.6) Any ICT standardization will be enforced by the ICT office. This has to be enforced by the responsible office to which IT office reports.

4.6.7) Copying software from the machines or any other modems is not allowed. All purchases of software require prior approval. Purchase of software should be recommended by IT before approval.

4.6.8) Installation of ECM software on non ECM equipment personal machines is not allowed. Purchases of software should be coordinated with IT office.

4.7 Hardware

4.7.1) Replacement of ICT equipment shall be undertaken on the basis of annual review of needs and the existing ECM policy on systematic capital budgeting. There should be a guideline in terms of duration say 3 or 4 years at which computers should be replaced.

4.7.2) All ICT hardware of ECM should be serially numbered and coded to facilitate asset identification and physical location. Commissions to provide commission codes for commission identification.

4.7.3) Disposal of obsolete or any ICT hardware shall be governed by existing ECM policy on fixed assets.

4.7.4) Maintenance of ICT equipment of ECM shall be undertaken through periodic maintenance contracts with reputable and recognized ICT firms. ECM shall be at liberty to assess the performance of any contracted firm and terminate the contract.

5.0) Rules of the thumb: Simple Do's and Don'ts

5.1) Always check flash disks or memory cards for viruses before use. This action will safeguard the ECM computers.

5.2) Do unto others as one would like to be treated in terms of the tone, diction and respect. Moreover, when one is courteous, chances of getting a required response are greater than a discourteous email.

5.3) Do keep your password secure and do not share accounts.

5.4) Staff should not leave his/her personal computer unattended to without logging off to avoid possible misuse in one's absence.

5.5) Do not attempt to gain unauthorized access to information or facilities to any computer.
5.6) Do not trade insults with other people with whom you disagree using the Internet.
5.7) Do not use ECM computer to access, download, write, publish or circulate any pornography and/or obscenities.
5.8) Do not, as an ICT user (ECM staff), under any circumstances engage in any activity that is illegal.
5.9) Do not take or place food or drinks close to ICT equipment to avoid possible contamination of the equipment.
5.10) Do not re-arrange how ICT equipment is plugged without advice from relevant ICT specialists.

6.0) Printers, telephone lines, facsimiles and photocopiers

All printers, telephone lines, facsimile machines and photocopiers are intended for use in the best interest of ECM. It is therefore incumbent upon all ECM personnel at whatever level to use the equipment responsibly. Excessive and irresponsible personal use of any of the equipment is strongly discouraged. On the other hand, ECM acknowledges circumstances that require prudent personal use particularly during emergencies.

6.1) General Computer use

6.1.1) Computers and laptops are primarily for office use, however laptops can be taken home for official use.
6.1.2) All peripherals such as scanners, printers, fax machines and speakers are strictly office equipment. These can be moved about after proper permission is granted by the Secretary General (or through the Head of Department).
6.1.3) Purchasing ICT equipment – procedures have to be followed: (SG) or Head of Department approval then specification by ICT Office then source quotations by Administration Department and afterwards IPC consideration & approval. IT standards recommend a minimum of latest version/generation computers as business computers and pre-loaded with professional versions of Microsoft windows and Microsoft office.
6.1.4) Disposal of life-expired equipment – an internal auction sale should be organized after obtaining an approval from the SG.

6.1.5) User responsibility for care and safe keeping of hardware (especially laptops, handheld Personal Digital Assistant PDAs) is very important.

7.0) Enforcement and discipline

7.1) It is incumbent upon all ECM personnel to protect the ICT infrastructure and facilities and users should immediately report to authorities or supervisors of any suspected acts of violation, breach in the security system or virus to facilitate further investigation.

7.2) Any ICT user found to have violated any provision of this ECM policy shall be liable to disciplinary action in accordance with the ECM Disciplinary Code and Grievance Procedure.

7.3) Any ICT user that breaches licensing and/or copyright provisions may in addition to being subjected to the laid down ECM Disciplinary Code and Grievance Procedure may be held personally liable for any damages to the license/copyright holder.

8.0) Revision of ECM ICT Policy

This ICT policy shall be reviewed and approved by the ECM after three years upon recommendation by the Social Communications and Research Commission or as determined by changes in the ICT world.