CATHOLIC SYRO-MALABAR EPARCHY OF GREAT BRITAIN

Issued by
The Bishop and The Curia
St. Alphonsa of the Immaculate Conception Cathedral
Parish St Ignatius Square,
Preston PR1 1TT

Registered Charity Number - 1173537

Data Protection Policy & Framework

Version 1.0

DOCUMENT CONTROL

Document Name	Version	Status	Author
Data Protection Policy & Framework	1.0	Draft	Data Protection Officer
Document objectives:	This policy supports the Catholic Syro-Malabar Eparchy of Great Britain to comply with Data Protection legislation GDPR/DPA 2018, achieving best practice in the area of Information Governance.		
Target audience:	The Clergy, member staff/volunteers who render their service to the Eparchy.		
Monitoring arrangements and indicators:	This policy will be monitored by the Eparchy's Data Protection Commission to ensure it is always updated with the latest legislative changes as and when this takes place.		
Approved and ratified by:	Approved by Eparchy's DPC Ratified by Executive Committee (The Curia)	Date: **June 2019** Date: **July 2019**	
Date issued:	June 2019		
Review date:	**July 2021**		
Author:	Data Protection Officer		
Owner	The Bishop and the Curia.		

Change Record

Date	Author	Version	Page	Reason for Change

Version Number: 1.0	Issue/approval date: June 2019
Status: Final	Next review date: July 2021

CONTENTS

1. INTRODUCTION

Organisations that process personal data need to comply with Data Protection requirements. In the UK, organisations that processed data up until 25 May 2018 adhered to then existing Data Protection Act which was passed in 1998. However, in 2016 the EU promulgated a new directive in the name of General Data Protection Regulation (GDPR) and asked all its member states to abide by May 25 2018. The EU also allowed a member specific adaptation of GDPR in certain areas (like child consent etc) and thus we have Data Protection Act 2018 as well for the UK. Therefore, in the UK GDPR requirements are read in conjunction with Data Protection Act 2018. Whether the UK exit from the EU or not, Great Britain will follow GDPR in conjunction with DPA 2018, when organisation process personal data within the UK.

This policy is important for the Eparchy because it will help the clergy, staff, people/volunteers who provide service to the Eparchy to understand how to look after the information the Eparchy has collected for processing and assure its members that their data is processed in accordance with the legislative requirements of the UK.

2. PURPOSE

Information is a vital asset. It plays a key part in ensuring the efficient management of religious service planning, resources and functions. It is therefore of paramount importance to ensure that information is carefully managed, and that appropriate policies and procedures are in place to support a robust governance framework for information management.

Data Protection/GDPR looks at the way the Eparchy handles information about its members, staff, volunteers, contractors etc with particular emphasis on personal and confidential information. Without access to information it would be impossible to provide any quality religious service. A robust governance framework needs to be in place to manage this vital asset, providing a consistent way to deal with the many different information handling requirements both at the corporate diocesan level and also at regional levels.

The aims of this document are to maximise the value of organisational assets by ensuring that information is:

- Held securely and confidentially;
- Obtained fairly and efficiently;
- Recorded accurately and reliably;

- Used effectively and ethically;
- Shared appropriately and lawfully

To protect the information assets from all threats, whether internal or external, deliberate or accidental, the Eparchy will ensure that:

- Information will be protected against unauthorised access
- Confidentiality of information will be assured
- Integrity of information will be maintained
- Information will be supported by the highest quality data
- Regulatory and legislative requirements will be met
- GDPR/Information Governance training will be available to Eparchy's clergy, staff/volunteers etc.

3. LEGAL COMPLIANCE

The Eparchy regards all identifiable personal information, including special category data as confidential data. The Eparchy will maintain policies to ensure compliance with Data Protection Legislation.

The Eparchy, when acting as a Controller, will identify, establish and record a condition for processing, as identified by the GDPR under Articles 6 and 9 (where appropriate), for each activity it undertakes. When relying on Article 6, 1 (a) 'processing is as per explicit consent' or when relying on Article 6, 1 (f) 'processing is necessary for the purpose of legitimate interest' vested in the Controller', or any other criteria relied under Article 6 (1), the Eparchy will clearly inform its members the legal basis used and record this on relevant records of processing.

In order to process both the categories of data (personal data and special category data) mentioned below (p.6), an organisation needs to comply with additional lawful bases. The church falls in to this category as it processes both the data types.

If an organisation processing Personal Data (Category 1), it has to abide by the following lawful bases which are in the article 6 of the GDPR:

a. Consent **(the church can rely on this to process at the time of membership)**

b. Contract

c. Legal Obligation

d. Vital Interest

e. Public Task

f. Legitimate Interest. **(the Church can rely on this to process)**

If an organisation is processing Personal Data as well as Special Category Data (1 & 2 categories mentioned below), it has to abide by following additional lawful requirements. These are in the article 9 (2) of GDPR.

4. SCOPE AND DEFINITIONS

The scope of this document covers

- All clergy and permanent Staff of the Catholic Syro-Malabar Eparchy of Great Britain and;
- All volunteers serving on behalf of the Eparchy in various capacities.

The Eparchy beliefs the need for an appropriate balance between openness and confidentiality in the management and use of data. It fully supports the principles of corporate governance and recognises its charity accountability, but equally places importance on the confidentiality of, and the security arrangements to safeguard information. The Eparchy also recognises the need to share information in a controlled manner. As such it is the responsibility of the Eparchy's trustees, member clergy, and volunteers to ensure and promote the quality of information and use information in accordance with Information Governance best practice.

In order to assist staff/volunteers with understanding their responsibilities under this policy, the following types of information and their definitions are applicable in all relevant policies and documents

Personal Data (derived from the GDPR)	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
'Special Categories' of Personal Data (derived from the GDPR)	'Special Categories' of Personal Data is different from Personal Data and consists of information relating to: (a) The racial or ethnic origin of the data subject (b) Their political opinions (c) Their religious beliefs or other beliefs of a similar nature (d) Whether a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1998 (e) Genetic data

	(f) Biometric data for the purpose of uniquely identifying a natural person (g) Their physical or mental health or condition etc.

5. PROCESSES/REQUIREMENTS

5.1 Fair Processing Notice (Privacy Notice)

Being transparent and providing accessible information to individuals about how you will use their personal data is a key element of GDPR. The most common way to provide this information is in a Privacy Notice. The Privacy Notice will enumerate the legal grounds for processing data as a data controller on behalf of the data subjects. The Eparchy has written and published the FPN on its website which lists the types of processing it does. The Eparchy will make every effort to make available the FPN in plain language and also make available to those people for whatever reason cannot view the Notice online, in hard copy.

5.2 Children under 13

The GDPR requires that parents or guardians must give permission for organisations to offer an online service in order to hold or process the personal data of those under the age of 16. However, under DPA 2018, the UK government has lowered this age to 13 if they see fit. In line with this requirement, the Eparchy will gain consent from children aged 13 and above if they are asked to share their person details to receive any online content it provides.

5.3 Volunteers and their Personal Email Addresses

Syro-Malabar church relies on volunteers to give time and energy to function. However, it will abide by the ICO's official standing that under **no circumstances it is good practice to use personal email addresses to work on sensitive information on church's behalf.** This is because the email provider will have no official relationship with the church (as a Data Processor would) and have no vested interest in the church as a Data Controller.

5.4 Subject Access Request

The Eparchy will maintain policies to ensure compliance with the Subject Access Requests as per requirements from Individual Rights obligations. Please refer to the Individual Rights (as mentioned below) in accordance with the General Data Protection Regulation (GDPR) and the Data Protection Act (DPA) 2018. The Eparchy will provide individuals who request access to their data which is held by the Eparchy within 30 days as opposed to 40 days under DPA 1998.

5.5 Data subjects' rights known as 'individual rights'

a. right to access any of their personal data held by the Eparchy (known as a Subject Access Request);

b. ask to have inaccurate personal data changed;
c. restrict processing, in certain circumstances;
d. object to processing, in certain circumstances, including preventing the use of their data for direct marketing;
e. data portability, which means to receive their data, or some of their data, in a format that can be easily used by another person (including the data subject themselves) or organisation;
f. not be subjected to automated decisions, in certain circumstances; and
g. able to withdraw consent when the Eparchy is relying on consent to process their data.

5.6 Pictures and Videos

Pictures and videos are not exempt from GDPR and is not designed to stop the data controller (the Church) from recording services or taking pictures of church events. However, the Eparchy will take utmost care as to how these images are stored and managed, whether moving or still. The Eparchy will not necessarily require consent to take a picture or video of someone inside the church, or at a church event, as most of the time this will count as a public place. The UK law allows anyone to take photos in a public place. However, if the person could have a reasonable expectation of privacy (for example, a support group, pastoral meeting or other more intimate setting) then the Eparchy in this instance will gain consent.

The Eparchy will take extra care with images or video which identify people as Christians, as this come under '**Special Category'** data. If the Eparchy is going to display these images, it will consider who is going to see them. GDPR allows churches to process special category data under the **'legitimate interest**' lawful basis, so long as they do not share the data outside the church body. In line with this, the Eparchy will not gain consent to display pictures or even videos which contain special category data inside the church. However, if the Eparchy wants to put the pictures/videos (live streaming) on its website or out in the public, it will gain consent from anyone who is identifiable as this is the case of broadcasting the images outside the church. However, this does not apply to people in the worship team (so say the priest, the alter servants, and the Trustees etc) who are working on behalf of the Eparchy, and are therefore representing the Data Controller.

5.7 Direct Marketing

Direct marketing means the communication (by any means) of any advertising or marketing material which is directed, or addressed, to individuals. It includes contact made by organisations to individuals for the purposes of promoting the organisation's aims. The Eparchy will comply with the rules set out in the GDPR, the Privacy and Electronic

Communications Regulations (PECR) and any laws which may amend or replace the regulations around **direct marketing**. This includes, but is not limited to, when we make contact with data subjects by post, email, text message, social media messaging, telephone (both live and recorded calls) and fax. Any direct marketing material that we send will identify 'Syro-Malabar Catholic Church' as the sender and will describe how people can object to receiving similar communications in the future. If a data subject exercises their right to object to direct marketing we will stop the direct marketing as soon as possible.

5.8 Transferring personal data outside the European Union (EU)

Personal data will not be transferred (or stored) outside of the European Union unless this is permitted by the GDPR. This includes storage on a "cloud" based service where the servers are located outside the EU. We will only transfer data outside the EU where it is permitted by one of the conditions for non-EU transfers in the GDPR.

6. INFORMATION SECURITY

The Eparchy will adhere to the Information Commissioners Office (ICO) guidance for reporting, managing and investigating Information Governance and Cyber Security Serious Incidents Requiring Investigation (IG SIRI) and as part of this, will review and maintain incident reporting procedures and monitor and investigate all reported instances of actual or potential breaches. Under Data Protection Legislation, where an incident is likely to result in a risk to the rights and freedoms of the Data Subject/individuals the Information Commissioner's Office (ICO) must be informed no later than 72 hours after the organisation becomes aware of the incident. The Eparchy will draw up a separate data breach procedure to report and investigate data protection breaches within its diocesan, regional and local mass centres.

7. INFORMATION QUALITY ASSURANCE

The Eparchy's **Executive Committee** (the Curia) with the help of **Data Protection Commission** (DPC) will maintain policies and procedures for information quality assurance and the effective management of records. Please see the Records Management Policy.

Priest in-charge from each **regional as well as mission centre** is expected to take ownership of, and seek to improve, the quality of information within their services. Wherever possible, information quality should be assured at the point of collection. Data standards will be set through clear and consistent definition of data items, in accordance with national standards.

8. NEW SERVICES/CHANGE TO EXISTING SERVICES

The Data Protection Officer should be consulted during the design phase of any new service, process or information asset and contribute to the statutory Data Protection Impact Assessment (DPIA) process when new processing of personal data or special categories of personal data is being considered. The Eparchy will maintain a DPIA framework that includes an approved template, guidance and supporting checklists.

9. ROLES AND RESPONSIBILITIES

The Eparchy has a responsibility for ensuring that it meets its legal responsibilities and for the adoption of internal and external governance requirements. The Executive Committee (the Curia) is also responsible for ensuring that sufficient resources are provided to support the requirements of the policy. The following are the hierarchical structure of Eparchy's various committees which will stand to make sure Data Protection Compliance is maintained in the management of church data.

9.1 Catholic Syro-Malabar Eparchy of Great Britain Executive Committee (the Trustees/the Curia)

It is the role of THE Executive Committee to define THE EPACHY'S policies in respect of Information Governance, taking into account legislative and legal requirements. The Executive Committee is also known as the 'Curia' is responsible for ensuring that sufficient resources are provided to support the requirements of the policy. The Curia is there to ratify the policies and procedures drafted and approved by the Data Protection Commission. It's remit is to make sure Data Protection compliance agenda is implemented throughout the various centres of the Eparchy.

9.2 Catholic Syro-Malabar Eparchy of Great Britain, Data Protection Commission (DPC)

The Eparchy's DPC is responsible for overseeing day to day Information Governance issues; developing and maintaining policies, standards, procedures and guidance; coordinating Data Protection matters across the Eparchy and raising awareness of Information Governance. The DPC is there to approve the policies and procedure for ratification by the Curia.

9.3 Catholic Syro-Malabar Eparchy of Great Britain, Regional Co-ordinators (Priest in-charge)

Regional co-ordinators are responsible for ensuring that the policy and its supporting standards and guidelines are built into regional church processes and that there is on-going

compliance. Part of this obligation is to ensure that all clergy, staff/volunteers are trained and made aware of confidentiality requirements and procedures. They are also responsible for carrying out annual audits of information and retention.

9.4 Catholic Syro-Malabar Eparchy of Great Britain, Mission Centres (Priest in-charge)

Priest in-charge in each mission centre is responsible for ensuring that the policy and its supporting standards and guidelines are built into local church processes and that there is on-going compliance. Part of this obligation is to ensure that all staff/volunteers are trained and made aware of confidentiality requirements and procedures. They are also responsible for carrying out annual audits of information and retention.

9.5 Syro-Malabar Eparchy of Great Britain, All Clergy, Sisters, Staff, Volunteers etc.

All **Clergy, Sisters, Staff, Volunteers and those people who give service on behalf of the Eparchy** are responsible for ensuring that they are aware of and comply with the requirements of this policy.

10. TRAINING

All clergy, staff, volunteers are required to comply with the Eparchy's data protection procedures, policies and that includes undergoing training as per requirements. The Eparchy will ensure that all clergy, staff and volunteers receive Information Governance training appropriate to their role, either a face to face training or through an on-line portal.

11. MONITORING COMPLIANCE AND EFFECTIVENESS

This policy will be monitored by the Eparchy's Data Protection Commission to ensure any legislative changes that occur before the review date are incorporated. The Eparchy's IG action plan, along with regular progress reports will be monitored by the Data Protection Commission and Executive Committee (the Curia).

12. MONITORING AND REVIEW

This policy will be reviewed biyearly, in accordance with Eparchy's programme of policy review, and may subject to change as per decision by the Data Protection Commission.

13. CONTACTS

Any queries regarding this Policy should be addressed to the Eparchy's Data Protection Officer, whose contact details can be found on the diocesan website (http://www.eparchyofgreatbritain.org/home/inner/3)

Complaints will be dealt with in accordance with the diocesan Complaints Policy. Further advice and information can be obtained from the Information Commissioner's Office at https://ico.org.uk/

14. ADDITIONAL REFERENCES AND DOCUMENTS

- The Information Commissioners Office
  https://ico.org.uk/for-organisations/guide-to-data-protection/whats-new/
- The National Archives
  https://www.nationalarchives.gov.uk/
- The Charity Commission
  https://www.gov.uk/government/organisations/charity-commission
- Catholic Sryo-Malabar Eparchy of Great Britain – Data Security Policy
  http://www.eparchyofgreatbritain.org/home/inner/3
- Catholic Syro-Malabar Eparchy of Great Britain - Records Management Policy
  http://www.eparchyofgreatbritain.org/home/inner/3

Appendix 1 – Definitions and Useful Terms

The following terms are used throughout this policy and have their legal meaning as set out within the GDPR. The GDPR definitions are further explained below:

Data controller means any person, company, authority or other body who (or which) determines the means for processing personal data and the purposes for which it is processed. It does not matter if the decisions are made alone or jointly with others.

The data controller is responsible for the personal data which is processed and the way in which it is processed. We are the data controller of data which we process.

Data processors include any individuals or organisations, which process personal data on our behalf and on our instructions e.g. an external organisation which provides secure waste disposal for us. This definition will include the data processors' own staff (note that staff of data processors may also be data subjects).

Data subjects include all living individuals who we hold or otherwise process personal data about. A data subject does not need to be a UK national or resident. All data subjects have legal rights in relation to their personal information. Data subjects that we are likely to hold personal data about include:

a) the members of Catholic Syro-Malabar Eparchy;

b) our employees (and former employees);

c) consultants/individuals who are our contractors or employees working for them;

d) volunteers;

e) tenants;

f) trustees;

g) complainants;

h) supporters;

i) enquirers;

j) friends and family

k) advisers and representatives of other organisations.

ICO means the Information Commissioners Office which is the UK's regulatory body responsible for ensuring that we comply with our legal data protection duties. The ICO produces guidance on how to implement data protection law and can take regulatory action where a breach occurs.

Personal data means any information relating to a natural person (living person) who is either identified or is identifiable. A natural person must be an individual and cannot be a company or a public body. Representatives of companies or public bodies would, however, be natural persons.

Personal data is limited to information about living individuals and does not cover deceased people. Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

Privacy notice means the information given to data subjects which explains how we process their data and for what purposes.

Processing is very widely defined and includes any activity that involves the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing can also include transferring personal data to third parties, listening to a recorded message (e.g. on voicemail) or viewing personal data on a screen or in a paper document which forms part of a structured filing system. Viewing of clear, moving or stills images of living individuals is also a processing activity.