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

Records Management Policy & Procedure

Version v.1.0

This document includes data that is **CONFIDENTIAL** and shall not be disclosed outside of the Catholic Syro – Malabar Eparchy of Great Britain and shall not be duplicated, used, or disclosed in whole or in part for any purpose other than to evaluate and implement procedures defined within this document.

Document Control Summary

Document Name	Version	Status	Author
Records Management Policy	1.0	Final	Data Protection Officer
Document objectives:	This policy supports the Catholic Syro-Malabar Eparchy of Great Britain's Records Management and Retention requirements to comply with data protection legislations - GDPR/DPA 2018.		
Target audience:	The Clergy, staff and volunteers of the Catholic Eparchy who are involved in the processing of personal data.		
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

CONTENTS

PAGES

1. INTRODUCTION

This policy sets out how **Catholic Syro-Malabar Eparchy of Great Britain** (herein after referred to as 'the Eparchy') will approach the management of its records. This policy is part of a Records Management Framework that includes additional procedure, guidance, training, audit and strategy. Our records management framework fits into the wider context of Data Protection Requirements.

All records (including email, hard copy and electronic documents) generated are the Eparchy's records collected and processed as part of its functions as a charity (Catholic Church) and must be kept in accordance with the following statutory guidelines:

- The General Data Protection Regulations 2018
- The Data Protection Act 2018
- The National Archives

2. SCOPE AND DEFINITIONS

This policy covers all Eparchy's charity activities (religious activities) and all information, irrelevant of the media being used to store the information. Corporate records in all formats (paper and electronic), active and inactive, held for use in the organisation, including:

Administrative (e.g. diocesan corporate, catechism services, regional centres' , mission centres, personnel, estates, finance and accounting, customer services and litigation) including e-mails, other communication tools and text messages.

Records management is the process by which an organisation manages all the aspects of records and information, from their creation through to their eventual disposal (Records Lifecycle). The aim of the policy is to ensure:

- **Accountability** – Records are adequate to account fully and transparently for all business actions and decisions, in particular to:
  - protect legal and other rights of staff or those affected by those actions;
  - facilitate audit or examination;
  - provide credible and authoritative evidence.

- **Accessibility** – Records can be located when needed and only those with a legitimate right can access the records and the information within them is displayed in a way consistent with its initial use, and the current version is identified where multiple versions exist.

- **Interpretation** - The context of the record can be interpreted i.e. identification of staff who created or added to the record and when, during which business process, and where appropriate, how the record is related to other records.

- **Quality** – Records can be trusted - are complete and accurate and reliably represent the information that was actually used in, or created by, the business process, and its integrity and authenticity can be demonstrated.

- **Maintenance through time** - so that the qualities of availability, accessibility, interpretation and trustworthiness can be maintained for as long as the record is needed, perhaps permanently, despite changes of format.

- **Security** – Records are secure from **unauthorised or inadvertent alteration or erasure, access and disclosure** are properly controlled and there are **audit trails** to track all use and changes in order to ensure that records are held in a robust format which remains readable for as long as records are required.

- **Retention and disposal** – Records are retained and disposed of appropriately, using consistent and documented retention and disposal procedures, which include provision for appraisal and the permanent preservation of records with archival value. The British Security Industry Association standard (BSIA) EN15713:2009 - Secure Destruction of Confidential Material must be adhered to when destroying confidential information

- **All are trained** – so that all Eparchy clergy, staff and volunteers are made aware of their responsibilities regarding records management.

3. PROCESSES/REQUIREMENTS

Records are Eparchy’s corporate memory, providing evidence to actions and decisions and representing a vital asset to support daily functions and operations. Records support policy formation and managerial decision-making and protect the interests of the Eparchy. They support consistency, continuity, efficiency and productivity and help deliver services in consistent and equitable ways.
The Eparchy operates within a Data Protection compliance environment. Failure to meet any relevant requirement could result in official sanction (from the ICO), reputation damage and even limits on what data and services we could provide as a charity (church).

The organisational benefits from good records management are:

- control and availability of valuable information assets
- efficient use of staff/volunteers time
- compliance with legislation and standards
- good utilisation of storage and server space
- a reduction in costs

- support the day to day parish function that underpins the delivery of a high quality service to our Eparchy members.
- maintain the integrity of the records
- meet legal requirements
- monitoring and audit cycles

Records Life Cycle	
Lifecycle Stage	**Description**
1. Planning	Our Curia (the trustees) together with the subject matter experts in the **Data Protection Commission** shall ensure that the Eparchy shall develop and implement policy, procedures and functionality to deliver records management strategy at the diocesan/corporate level as well as regional and mission centre levels.
2. Creation & receipt	This is where a record is created and saved which is the information received/created in the course of Eparchy's everyday ministry. We shall ensure that our records are properly captured into **approved filing systems**, that they are protected from **unauthorised access** or change, are allowed **only role based access** and **need to know basis** assigned the correct data classifications and are named following an agreed standard. The modalities on how this will be managed will be on a procedure document, incorporating specific needs of the records captured at the diocesan, regional, and mission centre levels.
4. Retention	We shall retain non-current and superseded records in our filing system to support on-going service needs and compliance requirements. Our disposal schedules shall govern how long records are retained. Retained records shall continue to be protected and accessible, with storage facilities meeting appropriate standards.
5. Disposal	Our records shall not be retained indefinitely. At the end of the agreed retention periods, records shall be disposed of and appropriate records maintained. In most cases this will mean controlled destruction; a small percentage of records will be flagged for permanent retention (e.g. baptism certificate details, parish membership details etc). and will be passed to the appropriate place of deposit (POD).

3.1 General Data Protection Regulations 2018 (GDPR)

Under the General Data Protection Regulations 2018 (GDPR) the definition of 'sensitive data' are classified broadly in to 2 categories – 'personal data', 'special category data'.

'**Personal Data'** is defined as: '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' (Article 4(1))

Special Category Data

As described in article 9 of the GDPR, special categories of personal data are Personal Data revealing:

a) racial or ethnic origin
b) political opinions
c) religious or philosophical beliefs
d) trade union membership
e) the processing of genetic data
f) biometric data for the purpose of uniquely identifying a natural person
g) data concerning health or data concerning a natural person's sex life or sexual orientation

There are various GDPR definitions relating to the management of information and records. For example, under Article 4;

- **'processing'** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- **'restriction of processing'** means the marking of stored personal data with the aim of limiting their processing in the future;
- **'filing system'** means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;
- **'data concerning religious believe'** means personal data related to the religious believe/affiliation of a natural person.

For information on categories of data and their assigned definition, please refer to Appendix 2 - Categories of data/information**.**

3.2 Information Quality

Our records are evidence of our activities: they may be required for litigation, governance, external audits, statutory enquiries and as a basis for decision making. Our records need to be:

- ✓ complete (in terms of having been captured in full)
- ✓ accurate (factually correct, legibly and assured as to the integrity of the record.)

- ✓ relevant (the degree to which the data meets current and potential user's needs)
- ✓ accessible (available when needed)
- ✓ timely (recorded and available as soon after the event as possible) alterations or annotations (must be clearly identifiable, traceable to the author and authorised by an appropriate Eparchy nominated person)

3.3 Electronic/Manual / Paper Records

Electronic records are created in one of two ways:

- Electronic records may start off as paper records and be converted into electronic records by scanning them. For example, many modern photocopiers can be used to scan documents into PDFs.
- However, most records are "born electronic" – that is, they are created on computer in the first place.

In either case, the electronic record will need to be given a clear file title and saved in the correct place

Documents should generally include the following information on the first page:

- A **clear title or subject line** – this can be included as a "Re:" line on a letter.
- A **clear date** – but if inserting the date in Microsoft Word do not tick the "update automatically" option, as today's date will then be shown whenever the document is opened (rather than the date when the document was actually created).
- A **version number** in cases where a document goes through a number of changes and the earlier copies are retained. Version numbers can be of two types:
- Version 2, Version 3 etc – where a major revision is made
- Version 2.1, Version 2.2, Version 2.3 etc – where a minor revision is made
- The **author** and the location (diocese/regional centre/mission centre) creating the document

Files should be carefully named so that the combination of file and folder name clearly indicates the contents. It is helpful to establish a series of naming conventions for particular types of documents. For example:

Minutes – meeting date in a recommended format (yyyy mm dd) and name of the group or committee, for example "2019 05 01 Eparchy Mission Committee Minutes" rather than "1 August.doc". Having year then month in number format in the file title means any file list on screen will be in a helpful and logical order.

Reports – date of report (in yyyy mm dd format), name for report and version number if applicable. For example, "2019 02 02 Eparchy's Communications Strategy v5.6.doc".

The following general points also apply when naming files and folders:

- Is there a recognised term for the subject? Use this in preference. Folder names should be the same as those used in your filing structure.
- Is the term likely to be recognised in the future? Try not to use current buzz words which may have passed out of use in the future when the folders have not. For the same reason, try not to use abbreviations unless they are very obvious.
- If the subject is highly sensitive, for example an investigation into child abuse, files and folders should be very carefully named. Whilst someone may not be able to access the record through security controls, if they are able to see the name, it could give enough sensitive personal data to expose your office to problems and potentially endanger the named individual.
- It is worth considering adding the filename and file path to the footer of every document you create once it has been saved, to enable anyone with a paper copy to identify what it is and where the electronic copy can be found.

Paper copies of records must be kept secure and should be stored in an appropriate locked filing cabinet, situated either in the parish office (diocesan/regional centres/mission centres) or designated records store on site, or in an approved off-site storage facility, so they are available and accessible to those who need them. These records should only be accessed by authorised individuals and should have role based access only.

3.4 Records Inventory

We shall use the Records Audit/Information Asset Register's to monitor and understand what collections of records and information we hold and note each documents retention period. We shall work towards organising our records into a Records File Plan that lists our church activities, and the records that they create, in a systematic and organised way.

3.5 Disposal Schedules and Legal Holds

We shall not retain all of our records indefinitely. Disposal is the process that
leads to records being destroyed or transferred elsewhere. It includes a record of what happened so that we can clearly show that we do not have the information any longer.

Disposal of any records shall be *held* if they pertain to an existing / emerging legal matter or request for information – this is known as a Legal Hold. An inventory of the retained records and the reason for the extended period of retention must be maintained.

Our records shall be retained and disposed of following agreed disposal schedules and procedures that are based on the National Archives and advises gained from subject matter experts pertaining to church activity needs. Disposal shall always be carried out following confidentiality and sensitivity requirements.

Most records should be **destroyed** after a given period of time, in accordance with the retention advice given in separate factsheets for, dioceses, parishes, bishops' offices and mission centres. The Eparchy will have a retention schedule based on the retention guidelines given (but likely to be adapted to local circumstances). This retention schedule should indicate the manner in which different types of records should be destroyed. For paper records, there are two options:

- A lot of records can be recycled, provided they do not contain confidential details such as names and addresses. Many local authorities will collect paper and cardboard for recycling, and commercial companies also provide this service for a fee.

- Confidential records, including those containing names and addresses, need to be shredded. This can be done using a shredder on site or by a commercial company. Such companies should provide a Certificate of Secure Destruction to show that the records have been shredded.

Records which need to be retained permanently as **archives** should be deposited with the Diocesan (Eparchy's) Record Office (the "DRO"),

Unilateral disposal of records, particularly if done contrary to disposal schedules or legal holds, is a serious breach of policy.

3.6. Storage and security of electronic records

The greatest risk to your records is misplacement, loss and unauthorised access. Consequently it is vital that we properly control access to and use of our records, whether they are held on in-house computer systems or in outsourced storage.

Storage of electronic records on in-house computer systems

In most cases electronic records will be stored on in-house computer systems. While mission centres or even regional centres may rely on a single standalone computer, Eparchy's bishops' office (diocesan) should have a computer network with file storage on a central server. This may be supported by an **Electronic Document and Records Management System (EDRMS)**, which is a specialist piece of software to manage electronic records in a shared network environment. If an EDRMS is in place, there should be clear procedures for its use. An EDRMS will only improve electronic records management if it is correctly used. It should be supported by a developed filing structure, along with clear procedures and practices for users to adhere to, including arrangements for regular maintenance.

In the absence of an EDRMS, the next best alternative is to store records on a **shared network drive**. This is far better than saving documents to a personal file space such as “my documents”, as records can readily be accessed by colleagues when required – better one copy in a shared drive than several all in personal drives or folders. Where necessary, access to shared folders can be limited to those who have a need to use the contents. This can be done on a folder by folder basis on the network drive. The alternative of password protecting individual documents to restrict access is not recommended, as passwords can cause serious problems if users lose them, leave or are away for a protracted period of absence. In these circumstances it is almost impossible to recover the contents..

The use of **portable storage devices** such as USB memory sticks should be strictly limited and avoided altogether for storing sensitive information (for example, names and addresses). This is because:

They are easy to lose. If a USB drive goes missing there is a risk that it will get into the wrong hands. This can be highly embarrassing or worse still, jeopardise the security of those individuals whose details are contained in the data on the memory stick. They can easily corrupt and become unreadable as their manufacturing quality varies greatly. They are a major transmitter of computer viruses.

As a general rule, original electronic records shall not be saved to ‘offline’ storage such as non-networked computer hard drives, USBs or optical media. In some circumstances e.g. anticipated limited network connection, volunteers/staff/clergy may need to save copies of records to encrypted devices such as a USB memory stick or a laptop. This is permissible if the Eparchy’s Data Security Policy is followed, and any new records / versions are saved to the approved storage location as soon as possible and subsequently deleted from the storage device.

3.7 Data Backups

All of our data including electronic records are ‘backed-up’ to offline storage in accordance with the relevant Backup and Business Continuity Plan. It is vital that ‘rescued’ records are complete copies and are not changed in any way, this includes embedded metadata e.g. date created, data last modified.

It is essential to make regular **backups** of your data, so that data may be restored following a disaster or the accidental deletion or corruption of data. Backups should be stored securely away from the location of the machine or system on which they were created, ideally in another building or at least in a different room in the same building. A parish may decide to buy an external hard disk drive, which are quite cheap and simply plug into a USB port. The disadvantage of this method is that you will have to actively remember to make a backup, so an alternative is to set up automatic backups via the free or cheap online storage offered by many broadband and email providers (see section on outsourced storage below). In larger offices, such as dioceses, the backup procedure will usually be managed by the IT department. However, the backup will only cover network drives – documents stored on local drives (such the <C> drive) are not backed up and are not secure!

3.8 New Technologies – Cloud and Collaboration / Sharing

The use of new technologies to improve working practices, process monitoring and collaboration is becoming increasingly popular. These are characterised by services such as cloud storage and collaboration spaces being held outside of traditional on-site technology infrastructure.

The requirements of this policy shall apply to such technology because they are handling our information and records. Assurances must be in place to ensure that data retention schedules are met and data is fully deleted, to include, back-up copies and 'other' structures that may refer to or directly reference the data, for example, a document index.

3.9 Email Records / Electronic Communication

Email is a key communication tool. The email service is designed as a communication tool and is not an appropriate solution for long term file storage. Therefore, all emails that are records of business activity and/or formal record of a transaction should be saved to an appropriately named folder on shared network drive. Keeping all emails will result in a significant storage burden to the Eparchy and information may become difficult to locate due to the size of files and attachments being stored.

4. ROLES AND RESPONSIBILITIES

Position or group	Description of Records Management Responsibility
Data Protection Commission Lead	Accountable for the proper and compliant conduct of records management across the organisation.
Data Protection Officer	The Data Protection Officer (DPO) is the person within the Eparchy who has been identified to support the role of the Data Protection Officer (DPO) as per the statutory requirements from GDPR/DPA 2018. This role has the responsibilities as set out in the GDPR guidance as responsible to feedback any Data Protection issues to the Data Protection Commission and Executive Management (the Curia) The DPO will ensure that where an incident is likely to result in a risk to the rights and freedoms of Data Subjects (the members/service users of the Eparchy), the ICO (Information Commissioner's Office) is informed no later than 72 hours after the organisation becomes aware of the incident. They will also be part of the Data Protection Impact

	Assessment process on behalf of all Eparchy function.
Eparchy Records Management Lead	Day-to-day operational management of the records management programme and framework. Conducting audits. Supporting and training staff on records keeping. Providing records management services to all regions/missions centres and volunteers of the Eparchy.
Information Asset Owners (IAO)	The role of the IAO is to understand what information is held, what is added and what is removed, who has access and why in their own area. As a result they are able to understand and address risks to the information assets they 'own' and to provide assurance to the Data Protection Commission Lead on the security and use of the assets. This role is de-facto rests with the priest in charge of the Regional Centres and Mission Centres, however this role can be delegated.
All Clergy/Staff/Volunteers	All Clergy, and those staff and volunteers working/rendering their service on behalf of the Eparchy, are expected to follow this policy and its procedures. This covers records in all formats (paper and electronic), both active and inactive

5. TRAINING

All Clergy, staff, and volunteers are required to comply with Eparchy's Data Protection Policies and therefore it is also import that all are trained to the appropriate level to handle confidential data.

6. MONITORING AND REVIEW

In compliance with Data Protection Legislative requirements, this policy will be reviewed bi-yearly. The policy review will take into account comments received from the Eparchy's Curia (Exec Committee), Data Protection Commission Lead, Data Protection Officer and Records Corporate Officer, and input from the Safeguarding Commission.

7. 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/

8. REFERENCES AND ASSOCIATED DOCUMENTS

- Information Commissioners Office (Data Protection Act 2018 and General Data Protection Regulation) – www.ico.gov.uk/
- National Archives (Public Records) – www.nationalarchives.gov.uk
- Government Security Classifications April 2014 - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251480/Government-Security-Classifications-April-2014.pdf
- Sryo-Malabar Eparchy of Great Britain – Data Protection Policy and Framework. http://www.eparchyofgreatbritain.org/home/inner/3
- Sryo-Malabar Eparchy of Great Britain - Data Security Policy. http://www.eparchyofgreatbritain.org/home/inner/3

Appendix 1: Key Records Management Requirements

Legislation / Standard	Compliance Requirement
General Data Protection Regulations 2018	Regulates the processing of personal data relating to living persons. Article 5 of the GDPR requires that personal data shall be: a) processed lawfully, fairly and in a transparent manner in relation to individuals; b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes; c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed; d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay; e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."
Data Protection Act 2018 (DPA 2018)	The Data Protection Act 2018 replaces the Data Protection Act 1998 and legislates to an equivalent to the GDPR but includes national derogations not covered by the GDPR. The DPA 2018 should be read in conjunction with the GDPR.

Appendix 2: Protective Marking Scheme

<table>
<tr><td colspan="2">Please note that the categories of data/information listed below, will be used or referred to in all SM Eparchy of Great Britain Polices. The purpose of this approach is to ensure a consistent approach is adopted.</td></tr>
<tr><td><b>Personal Data</b> (derived from the GDPR)</td><td>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</td></tr>
<tr><td><b>'Special Categories' of Personal Data</b> (derived from the GDPR)</td><td>'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
(h) Their sexual life</td></tr>
<tr><td></td><td></td></tr>
</table>