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 Security Policy

Version 1.0

DOCUMENT CONTROL

Document Name	Version	Status	Author
Data Security Policy	1.0	Final	Data Protection Officer

Document objectives:	This policy supports the Catholic Syro-Malabar Eparchy of Great Britain to comply with data security in line with requirements from data protection legislation - GDPR/DPA 2018.	
Target audience:	The Clergy, staff and volunteers of the 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

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

CONTENTS

1. INTRODUCTION

Organisations that process personal data needs 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 countries to abide by May 25 2018. 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, and volunteers who provide service to the Eparchy to understand how to look after the information the Eparchy has collected and assure its members that their data is processed in accordance with the legislative requirements of the UK.

2. PURPOSE

Information, whether in paper or electronic form, is of high importance to the Catholic Syro-Malabar Eparchy of Great Britain for its services and so should be kept secure. Therefore the organisation must ensure that the information is properly protected and is reliably available.

Information Security is primarily about people (the data subjects) but is facilitated by the appropriate use of technology. The benefits of this policy and associated guidance are:

- Assurance that all EPARCHY'S information is being managed securely and consistently and in line with its other associated policies and guidance.
- Assurance that EPARCHY is providing a secure and trusted environment for the management of information used in delivering its religious services.
- Clarity over the personal responsibilities around information security expected of the clergy, staff, trustees, volunteers etc. when rendering services/working for EPARCHY.
- Demonstration of best practice in Information Security.
- Assurance that information is accessible only to those authorised to have access.

The requirements within this Policy are driven by the Data Protection Legislation covering security and confidentiality of personal information, including the General Data Protection Regulation 2016 and the Data Protection Act 2018.

3. SCOPE AND DEFINITIONS

This policy applies to all EPARCHY clergy, staff, trustees, volunteers, contractors/temporary contractors, third party suppliers, voluntary organisation and anyone duly authorised to view or work with EPARCHY information.

The purpose of this Data Security Policy is to protect, to a consistently high standard, all information assets, including all Eparchy/parish records and other corporate information, from all potentially damaging threats, whether internal or external, deliberate or accidental.

This Information Security Policy covers all forms of information held by the EPARCHY, including
but not limited to:

- This may include Catholic Syro-Malabar members (parishioners), volunteers, clergy, employees, contractors, suppliers and other third parties
- Organisational, Business and Operational Information.

This Information Security Policy applies to all aspects of information handling, including, but not limited to:

- Structured Record Systems – paper and electronic
- Information Recording and Processing Systems – Paper, Electronic, Video, Photographic and Audio Recordings.
- Information Transmission Systems, such as fax, email, portable media, post and telephone.

What is Personal Data?

As described in part 1, subsection 3 of the Data Protection act 2018

(2) "Personal data" means any information relating to an identified or identifiable living individual

(3) "Identifiable living individual" means a living individual who can be identified, directly or indirectly, in particular by reference to—

(a) An identifier such as a name, an identification number, location data or an online identifier, or

(b) One or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual

What are "Special Categories of Personal 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
h) data concerning a natural person's sex life or sexual orientation

Under the **Data Protection legislation** an organisation can only process or have access to personal data if:

- An appropriate condition for processing (GDPR Article 6 and Article 9) and where necessary a supporting lawful basis has been identified and documented in a statutorily required Data Protection Impact Assessment (DPIA) or,
- Explicit consent has been obtained from the individual or,
- The data has been anonymised or pseudonymised in line with Data Protection legislation requirements; or
- The data is in respect of safety, safeguarding or in the public interest.

Cyber Security

Information and Cyber Security concerns the comprehensive risk management, protection and resilience of data processing and the digital networks that connect them. The Eparchy will put in place a robust system and procedures to manage Cyber Security requirements throughout all of its IT estates.

4. PROCESS REQUIREMENTS

This Information Security Policy will achieve a consistent approach to the security management of information throughout the EPARCHY and will aim to deliver uninterrupted services, and minimise both the likelihood of occurrence and the impacts of information security incidents.

- Those working for the EPARCHY shall accept full responsibility for the security of information and information assets which are issued to them, taking necessary precautions to avoid loss, theft or damage. Information should not be left unattended in a public place or left in vehicles either on view, unattended or overnight.

- Access to information shall be restricted to users who have an authorised need and access has been approved by the relevant **Information Asset Owner (**IAO) who are the:
    - Eparchy's diocesan level in-charge (Proto Cyncellus)
    - Eparchy's co-ordinator at regional level (priest in charge)
    - Eparchy's mission centre level in-charge (priest in charge)

- All devices, including computers, portable **devices - such as laptops, memory sticks, palm tops, mobile phones etc** that are intended for use with personal or special category information belonging to the EPARCHY must be supplied and supported by EPARCHY.
- Each Regional Centre is responsible for holding an information asset register which details the **specification, user and location** of the asset. IT equipment will be security marked and its serial number should be recorded. It is the responsibility of the EPHARCHY'S regional co-ordinator to update and maintain the asset register in the template provided.
- If the Eparchy has a 'Bring Your Own Device' Policy, commonly known as BYOD, ensure staff, clergy and volunteers must adhere to it.
- If Eparchy data has to remain temporarily on a device, ensure that it is backed-up daily onto a secure external medium such as an **encrypted memory stick** provided by the Eparchy – but this should not become normal practice.
- Where it is necessary for Diocese/Eparchy data to be held on a personal device, delete it as soon as possible once it is no longer required. This includes information contained within emails.
- **Password Management** – All devices should have passwords, passcodes, passkeys or biometric equivalents (as applicable) set up. These must be of sufficient length and complexity for the particular type of device.
- **E-Mail Management -** The Eparchy should have its own e-mail account to correspond Eparchy data. Personal e-mails **must** not be used for transferring personal/special category data processed by the Eparchy. The Eparchy also should not use personal e-mails to do any of its own functions. However, the Eparchy can make use of private e-mails for communication purposes, provided explicit consent is gained from the individuals prior to being added to the circulation list. It is always required to use 'BCC' function (Blind Carbon Copy) other than 'CC' whenever private e-mails are used in the mailing list for correspondence. When a message is blind carbon copied, neither the main recipient nor the **Bcc**'d recipients can see the addresses in the "**Bcc**:" field. Blind carbon copying is a useful way to let others see **an e-mail** you sent without the main recipient knowing.
- Agreed contracts with third party IT suppliers working for and on behalf of EPARCHY must be clearly agreed and signed.
- **Use of Social Media –** The Eparchy can make use of social media (Facebook, twitter, WhatsApp) for its charity service as part of communication; however, personal data should not be stored/used or transferred over any of these mediums. Social media cannot be used for Eparchy's everyday functions as well as the Eparchy has no valid

legally binding contract these providers. The Eparchy can make use of social media for communication purposes; however, explicit consent needed to be gained before the user can join (can withdraw this consent any time).

- All IT equipment used by the Eparchy is **encrypted and protected** by countermeasures and management procedures to protect against the threat of **malicious software**. Users shall not install software on the Eparchy's IT property without permission from the IT Services.
- An annual mapping exercise of **data assets** within the Eparchy (diocesan centre), in each of the Regional Centre, Mission Centres will be undertaken. There will be also a **data flow register** completed for the whole of the Eparchy for the data it receives and sent out to third parties for accountability. These exercises will allow any information risks to be identified by each centres and appropriate action to mitigate those risks should be taken. It is the responsibility of the IAOs (Information Asset Owners who is the priest in charge at the respective place) to ensure that this takes place.

5. SECURE TRANSFER OF INFORMATION

For the secure transfer of bulk electronic information (e.g. children data for catechism, members' names on the registry, etc.) a secure file transfer function should be used and should have approved levels of encryption. Private e-mails should not be used for transferring personal/special category data. The eparchy will ensure that paper information is securely transferred by following adequate '**transfer of personal information procedures', '**records management procedures and processes. The EPARCHY should promote a 'paper light' environment through use of electronic devices to transform information to a secure electronic form.

6. DATA SECURITY BREACHES – REPORTING & INVESTIGATIONS

All individuals who are involved in the processing of personal data on-behalf of the Eparchy, **the trustees, clergy, staff and volunteers**, are responsible for ensuring that no potential or actual security breaches occur as a result of their actions. The Eparchy will investigate all suspected / actual security breaches internally. A personal data breach is defined under the Regulation as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".

As and when a data breach is reported or come in to light within a regional centre/mission centre, this needs to be reported to the priest in-charge (Asset Owner) as soon as possible for internal investigation. The incident needs to be logged on to the incident management log or system by either the person reporting it or by the priest in-charge at the respective regional/mission centres. The priest in-charge will also need to escalate this to the Eparchy's Data Protection Officer if it is judged to be a serious breach. The DPO has the responsibility

to inform the ICO within 72 hours about the incident “unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons". In addition, where there is a high risk of damage arising to the data subject then the data subjects must be informed directly without undue delay for further investigation.

All incidents will be investigated immediately once logged for actions taken, lessons learned and mitigation plans to eliminate reoccurrence.

7. INFORMATION DISPOSAL

All IT assets must be disposed of in accordance with the standard disposal of confidential waste procedure. This includes removable computer media, such as tapes and disks. All data storage devices must be purged of personal and confidential data before disposal. Where this is not possible, the equipment or media must be destroyed by a technical waste service provider. For further information, please contact EPARCHY’S IT services. Printed matter/hard copy files should be confidentially destroyed using an appropriate method such as shredding. Where the Eparchy has large quantities of confidential waste for disposal, this should be done through a secure shredding contract or the local authority can help in this regard.

8. NEW PROCESS OR CHANGE TO EXISTING PROCESS

Under the General Data Protection Regulations 2016 the completion of a **Data Protection Impact Assessment (DPIA)** is a statutory requirement where there is change to an existing processing or a new processing involved which is deemed to pose high risk to the rights and freedom of the data subjects. The Eparchy’s DPO has the mandate to make sure a DPIA is completed if the new project in question involves high risk to individual’s privacy. Under section 157 of the Data Protection Act 2018, the ICO is able to impose a penalty for failing to complete a DPIA when it is mandated to do so under Article 35 of the GDPR. The maximum amount that can be imposed is 10 million Euro’s or 2% of total annual worldwide turnover in the case of an undertaking or group of undertakings.

9. ROLES AND RESPONSIBILITIES

EPARCHY Senior Information Risk Owner (SIRO) – The Bishop

The Senior Information Risk Owner has overall responsibility for **Data Security** within the organisation that also has allocated lead responsibility for the organisation’s information risks and provides the focus for management of information risk at executive management (the curia) level. The Bishop takes this responsibility on behalf of Syro-malabar Eparchy of Great Britain. The SIRO should make sure that information risk is being managed appropriately and effectively across the Eparchy structure (diocesan, regional and mission centre levels) and for any services contracted by the Eparchy.

Data Protection Officer (DPO)

The Data Protection Officer (DPO) has the responsibilities as set out in the GDPR guidance and is responsible to ensure that where an incident is likely to result in a risk to the rights and freedoms of Data Subjects, 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 (DPIA) process on behalf of the Eparchy. Catholic Syro-malabar Eparchy has appointed a DPO as per GDPR requirements in this regard.

The Data Protection Commission (DPC)

The Data Protection Commission is responsible for ensuring that the Data Protection compliance agenda is implemented throughout the Eparchy. The team is also responsible making sure the Eparchy is compliant on Data Protection matters. The commission also will draft policies and procedure for approval and adaptation. The Commission will also discuss and approve Data Protection Impact Assessments (DPIAs). The Commission also will support the organisation in investigating Serious Incidents Requiring Investigation (SIRIs) in their periodical meetings, offer advice and ensure the Eparchy, with its regional and mission centres, complies with legislation, policies and protocols.

The Eparchy Information Asset Owners (IAO)

The SIRO is supported by Information Asset Owners (IAOs). The role of the IAO is to understand what data and 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 SIRO on the security and use of the assets. Within the Eparchy, each regional co-ordinator and mission centre leads (priests' in-charge) will take the responsibility as the IAO.

IT Security Support

The Eparchy has appointed an IT Security lead to implement and look after its IT assets/estates throughout the Eparchy.

Responsibilities of the IT Security lead include:

- Maintaining and giving/terminating user access to IT systems network and functions across the Eparchy. Acting as a central point of contact on IT security within the organisation (diocesan, regional and mission centre levels) and for external organisations that has entered into an agreement for the provision of IT services by the Eparchy. Implementing an effective framework for the management of security. Assisting in the formulation of Information Security Policy and related policies.

- Making sure that all IT systems, including desk tops, laptops, palm tops, removable storage equipment's' etc. that are in use by the Eparchy is encrypted to the required standard level.
- Co-ordinate IT security activities particularly those related to shared information systems or IT infrastructures. Liaise with external organisations on IT security matters, including representing the organisation on matters of IT infrastructure within the Eparchy.
- Advising users of information systems, applications and Networks of their responsibilities.
- Maintaining the security of the IT infrastructure network by installing and updating with latest patch/version of antivirus software. Also doing end point penetration testing periodically to withstand cyber security/hacking attacks.
- Creating, maintaining, giving guidance on and overseeing the implementation of IT Security which also includes assisting in completing DPIAs if there is a new procurement or change to existing IT systems involved.

10.TRAINING

The Eparchy is to ensure all individuals who deal with personal/special category data to receive basic Data Protection Training appropriate to their role through either a phased manner face to face training or through a custom made material made available through MS power point, made available on Eparchy website or otherwise. The Eparchy's Data Protection Commission is to make sure individuals who handle personal data are appropriately trained as for compliance.

11.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.

12.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/

13. 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

- Sryo-Malabar Eparchy of Great Britain – Data Protection & Framework Policy
  http://www.eparchyofgreatbritain.org/home/inner/3
- Syro-Malabar Eparchy of Great Britain - Records Management Policy
  http://www.eparchyofgreatbritain.org/home/inner/3