



CATHOLIC SYRO-MALABAR EPARCHY OF GREAT BRITAIN

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

Registered Charity Number - 1173537

Bring Your Own Device (BYOD) Policy

Version 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

Document Name	Version	Status	Author
---------------	---------	--------	--------

BYOD Policy	1.0	Final	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 in relation to the use of own IT equipment by its staff/clergy/volunteers while rendering their services to the Eparchy.		
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 DP Commission Ratified by Executive Committee (The Curia)		Date: Dec 2024 Date: TBC
Date issued:	Dec 2024		
Current review date and next review date:	Dec 2024 & Dec 2027 respectively.		
Author:	Data Protection Officer		
Owner	The Bishop and the Trustees		

Change Record

Date	Author	Version	Page	Reason for Change

INTRODUCTION

Organisations that process personal data need to comply with Data Protection legislative requirements. In the UK, organisations that process personal data must adhere to the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, the Common

Version Number: 1.0
Status: Draft

Issue/approval date: Dec 2024
Next review date: Dec 2027

Law on Duty of Confidentiality, and other relevant data protection legislation. The Catholic Syro-Malabar Eparchy of Great Britain (henceforth called, '**the Eparchy**'), collects and processes the personal data of individuals as a data controller and thus must conform to legislations such as those mentioned above. The UK GDPR is an adopted version of GDPR, which was EU promulgated, and the UK government domiciled it upon exiting the EU in 2020. This policy is important for the Eparchy because it will help the clergy, staff, and volunteers who provide service to the Eparchy to understand the requirements of complying with data protection laws when using own IT equipment when connecting to the Eparchy network and data when rendering their services to the Eparchy.

The Eparchy has a responsibility to safeguard the information that has been provided to it by its members, faithful and various other organisations to carry out its religious activities. To do this, we need to make sure that:

- the requirements of UK laws on data protection are being met
- the Eparchy's own Data Privacy and Information Security policies are being followed
- where third party data is being used, the requirements of the data owners are being followed

The Eparchy recognises that users may wish to use their own devices (IT equipment) to access Eparchy data and use Eparchy applications as part of flexible working arrangements. This policy outlines the responsibilities of both the device owner and the Eparchy.

POLICY SUMMARY

This policy covers use of a device (IT Equipment) owned by CLERGY, STAFF AND VOLUNTEERS other than the devices provided by the Eparchy (for example, personal devices) to access Eparchy network and data – commonly known as Bring Your Own Device (BYOD).

You must comply with the whole policy, but in summary:

- **Conform to Eparchy Policies** - If you have accepted the Eparchy's data protection policies, adhere to the confidentiality agreement and your device meets certain criteria, you may access Eparchy network and data from a personal device.
- **The Eparchy retains control of the data**, and as part of this agreement you accept that the Eparchy can erase data from your device if it is found that Eparchy data is stored within the IT equipment's local drive.
- **You must tell the Eparchy immediately** if your device is lost, stolen, infected with malware or the security of the device is otherwise compromised
- **The Eparchy only supports the use of personal devices** to log in to Eparchy's online network services and it is **not meant to store any Eparchy data locally in the devices local drive**.
- Compliance with this policy is part of your service contract with the Eparchy – this applies to Clergy, Staff and Volunteers rendering services to the Eparchy.

Prohibited services and data

The Eparchy and its partners reserve the right to prohibit use of personally owned devices (BYOD) for accessing certain category of services and data (the user will be notified of a such data time to time) as necessary.

Who does the policy apply to?

This policy applies to all persons (Clergy/Staff/Volunteers) who connect or intend to connect a device (an IT equipment) not owned by the Eparchy to its network and data.

The Eparchy's responsibilities

As the data controller, the Eparchy is responsible for ensuring that all processing of personal data which is under its control remains in compliance with UK law. Additionally, the Eparchy receives data from other organisations which may be restricted by their security policies with which we have to comply. The Eparchy must also remain mindful of the personal usage of such devices and the privacy of the individual. Technical and organisational measures used to protect the Eparchy owned data must remain proportionate to the risks and consider rights of an individual to privacy. Decisions on these matters will be made via the Eparch's internal governance routes.

Rights, privileges and responsibilities

The use of a personally owned device in connection with Eparchy services is a privilege granted to device owners. The Eparchy reserves the right to revoke these privileges without notice.

Every Clergy, Staff, and Volunteer must read and understand this policy before connecting your device to access Eparchy information.

You must complete the Eparchy's data protection training on Data Protection, Information Rights and Cyber Security, and accept its IT Security/Acceptable Use Policy before being provided access to Eparchy information from your personal device.

The Eparchy remains the **data controller** for all data held on BYODs.

Disciplinary and/or criminal action may be taken if a breach of policy or law occurs. Compliance with this policy is part of your Clergy/Staff/Volunteer service contract with the Eparchy.

As the device owner, you carry specific responsibilities, as listed below:

- You will not lend anyone your device to access Eparchy information or use Eparchy infrastructure
- Should you decide to sell, recycle, give away or change your device, you will inform the Eparchy's IT service. **Do not allow the device to leave your possession until you have informed Eparchy data has been wiped (if applicable)**
- Every BYOD device must have log-in password set before unlocking for use.
- You are responsible for the safekeeping of your own personal data.
- We recommend that you secure and encrypt your phone appropriately using the facilities on the device, and that you have an up-to-date malware scanning solution installed (anti-virus). All users are expected to use their device in an ethical manner.

Which devices are covered?

Current devices approved for Bring Your Own Device use are listed below along with the minimum system requirements:

- Android Smart Phones and Tablets that are supported currently.
- iOS iPhones and iPad (note that Apple do not guarantee support for any version other than the latest).
- MacOS devices (note that Apple to not guarantee support for any version other than the latest update).
- Windows 10 devices that are currently supported.

It should be noted that as technology improves, and newer versions of operating system are introduced by vendors or vulnerabilities are discovered in existing operating systems this list is subject to immediate change.

Which IT services are available?

Currently, the IT Services available and covered by policy are:

- Emails and file access through their online Drives (Google Drive/One Drive) using the Microsoft Office suite and Google Classroom.
- calendars
- tasks
- telephony, meetings and instant messaging
- For the mobile device, collaboration and group discussion through Zoom & MS Teams
- Home Wi-Fi

Who monitors and implements the policy?

Eparchy's IT in conjunction with the Data Protection Commission will manage the BYOD policy.

What support will Eparchy IT provide?

The Eparchy IT will not support or maintain any personal device. Furthermore, the Eparchy will not cover any damage to the device or any loss of the equipment owner's personal data that may occur because of its use for the Eparchy. It is recommended that device owners insure their device as part of their home contents insurance or via a specific mobile device insurance scheme.

If a security incident should occur

A security incident is defined as **any** event that could compromise information security. Some examples: your device is lost or stolen, someone else gains access to your password/passcode, your device becomes infected with malware. If a security incident should occur, you are required to inform the Eparchy (Priest in-charge of the Parish/Mission/Proposed mission) or the relevant contact **immediately. You are also required to complete the incident form (data breach form)** with details of the Eparchy. Note that not reporting security incidents is a breach of the IT Security /Acceptable Use Policy.

Guidelines for acceptable behaviour

Device owners are expected to behave in accordance with the Eparchy's best practice and confidentiality requirements. Be aware that any personal device used for Eparchy's work may be subject to discovery in litigation. This means that it could be used as evidence in a lawsuit against the Eparchy. Your data could be examined not only by the Eparchy but also by other parties in any legal action.

If you leave the service with the Eparchy

As part of the leaver's process, your access to the Eparchy infrastructure and applications will cease and any Eparchy data on the equipment will need to be handed over to the Eparchy for retention and destruction.

The Eparchy release of liability and disclaimer statement

The Eparchy hereby acknowledges that the use of a personal device in connection with Eparchy service carries specific risks for which you, as the device owner and user, assume full liability. These risks include, but are not limited to, the partial or complete loss of data as a result of a crash of the OS, errors, bugs, viruses, and/or other software or hardware failures, or programming errors which could render a device inoperable.

Device owners bring their devices to use at the Eparchy as their own risk. Device owners are expected to act responsibly with regards to their own device, keeping it up to date and as secure as possible. It is their duty to be responsible for the upkeep and protection of their devices.

The Eparchy is in no way responsible for:

- personal devices that are broken while at work or during work-sponsored activities
- personal devices that are lost or stolen at work or whilst undertaking work-related activities for the Eparchy.
- maintenance or upkeep of any device (keeping it charged, installing updates or upgrades, fixing any software or hardware issues)

Finally, the Eparchy reserves the right, at its own discretion, to remove any

Eparchy supplied applications from your personal device as a result of an actual or deemed violation of the Eparchy's BYOD Policy.

=====

DO NOT COPY