Bringing people closer to Jesus Christ through His Church

Catholic Diocese of Portsmouth

Diocesan Operating Procedures
Data Protection

"But everything must be done in a proper and orderly manner."

1 Corinthians 14:40

Issued by:

The Bishop of Portsmouth and the Catholic Diocese of Portsmouth
St Edmund House
Bishop Crispian Way
Portsmouth
PO1 3QA

England Registered Charity No. 1199568
Jersey Registered Charity No. 381
Guernsey Registered Charity No. CH263

Contents

INTRODUCTION

The Diocesan Operating Procedures (DoPs) are provided as guidance to managers and to employees on how a wide range of issues should be managed in relation to the Data Protection Act 2018 (DPA) and the UK General Data Protection Regulation 2018 (UK GDPR).

The underlying rationale to DoPs is to provide a framework of policies and procedures which provide a way of working within the concept of fairness and justice.

It also provides employees, volunteers and line managers with relevant forms, letters, and documents in a series of appendices for use in the appropriate circumstances.

Policies provide general and practical advice as well as guidance on a range of issues to ensure all employees (and volunteers) act appropriately as required by the Diocese and in adherence to relevant legislation.

Procedures support and supplement the policies by giving a step- by-step account of specific arrangements that apply in particular circumstances.

Forms and Guidance notes are also provided throughout relating to the policies and procedures.

Please note that these policies and the accompanying procedures and forms are for guidance only. They do not have contractual status as they may be amended from time to time

APPROVALS

The signatures below certify that this document has been reviewed and accepted demonstrating that the signatories are aware of all requirements contained herein and are committed to ensuring their provision.

	Name	Signature	Position	Date
Prepared by	David Lawes		Head of the Dept. for Administration	2017
Reviewed by	Sheilah Mackie		Partner, Blake Morgan Solicitors	2017
Prepared by	Lucy Sawyer		Administrative Services Manager	2018
Reviewed by	Mark James		Data Protection Officer	2020
Reviewed by	Maria Devine		Governance Manager	Jul 2021
Reviewed by	Karena Fulford		Head of People, Governance, and IT	Jul 2021
Reviewed by	Dave Little		Interim IT Manager	2021 Aug
Reviewed by	Mark James		Data Protection Officer	18 Aug 2021
Approved by			SLT	2022 Jan
Approved by			FAR	2022 Jan
Approved by			Trustees Board	2022 Feb

Reviewed by				

AMENDMENT RECORD

This document is reviewed to ensure its continuing relevance to the systems and processes that it describes. A record of contextual additions or omissions is given below.

Page No.	Context	Revision	Date
All	Entire policy reviewed.		Jun 2021
Title Page	New Charity name and number updated		Jan 2023

FOREWORD

God's Church here in the Catholic Diocese of Portsmouth is formed of many and varied communities, held together in the same Truth of Christ both in doctrine life and worship. We need common operating procedures across the Diocese to ensure compliance with the needs of both canon and civil law. In addition, and especially in the light of the church's call to the work of new evangelisation, we need to ensure harmonised collaboration. We have a responsibility to ensure that people, buildings, and money are treated carefully allowing us to perform our duties "with the diligence of a good householder" (Canon 1284§1).

These Diocesan Operating Procedures (DoPs) have the status of particular law for the Catholic Diocese of Portsmouth. They must be understood and followed in the broad areas of human resource, schools, buildings, and finance.

I am very grateful to all those who have compiled these procedures and ensure their regular review and updating.

In Corde Iesu

+Bishop Egan
Bishop of Portsmouth

TERMINOLOGY

Throughout this DoP, the Catholic Diocese of Portsmouth will be referred to as **'the Diocese'**. This expression shall include any representative acting for or on behalf of the Diocese Trustees, for example HR, Line Managers or any other representative appointed to carry out work on behalf of The Catholic Diocese of Portsmouth.

Throughout this DoP the expression, **'Line Manager'**, will be used which may be referring to a Co-ordinating Pastor/Parish Priest/Head of Department or any other person with line management responsibilities.

This DoP is subject to changes brought about by relevant legislation, regulations, and changes in best practice. Any changes and amendments that may be made to this document will be brought to the attention of line managers and Parishes. They will then be guided towards the current version online:

Policies and Documents | Portsmouth Diocese
Guidance is available from the relevant department in the Curia:
Governance Team: Tel. 02394 216 500

THE BISHOP'S VISION

The Bishop of Portsmouth and the Trustees are fully aware of their duty of care to all our employees, and to anyone who works within the Catholic Diocese of Portsmouth.

Diocesan policies must comply fully with the current statutory regulations concerning employment, data protection, health and safety and the many regulations which relate to employees and to the workplace.

However, it is our aim that our policies do more than comply with regulations.

It is our aim that our policies provide a framework of guidance for all who work within the Diocese: guidance to support and encourage us all in our work, to enable a working environment that is based on co-operation, respect for each other's gifts, tolerance and support for each other's limitations, and above all, fairness and justice in our dealings with each other.

Please read these policies, become familiar with the procedures and the forms, and help us to ensure that our work together fulfils our aims of respect, tolerance, and fairness.

Data Protection Policy

Glossary Of Terms

"Diocese" means the Catholic Diocese of Portsmouth.

"Data Controller" has a specific meaning within the General Data Protection Regulation. It means a person, organisation or body that determines the purposes for which, and the manner in which, any Personal Data is processed. The Diocese is the sole Data Controller, and this includes all Processing of data that is carried out by any Diocese member including curial offices, parishes, departments, and agencies. The Diocese, as Data Controller, is responsible for complying with the Data Protection Rules and establish practices and policies in line with them.

"Data Processor" means any person, organisation or body that processes personal data on behalf of and on the instruction of the Diocese (e.g., a contractor). Data processors act on the instructions of the Data Controller and have a duty to protect the information they process by following the Data Protection Rules.

"Data Subject" means a living individual about whom the Diocese processes Personal Data and who can be identified from the Personal Data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their Personal Data and the information that the Diocese holds about them.

"Personal Data" means any information relating to a living individual who can be identified from that information or in conjunction with other information, which is in another's possession, or is likely to come into possession. Personal Data can be factual (such as a name, address, or date of birth) or it can be an opinion (e.g., a performance appraisal). It can even include a simple email address. A mere mention of someone's name in a document does not necessarily constitute Personal Data, but personal details such as someone's contact details or salary (if it enabled an individual to be identified) would fall within the definition. An item of personal data can belong to more than one data subject if they are both/all identifiable.

"Processing" means any activity that involves use of Personal Data. It includes obtaining, recording, or holding the information or carrying out any operation or set of operations on it, including organising, amending, retrieving, using, disclosing, erasing, or destroying it. Processing also includes transferring or disclosing Personal Data to third parties.

"Special Categories of Personal Data" (previously called *sensitive personal data*) means information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health or condition, or

data concerning a natural person's sex life or sexual orientation. It also includes the processing of genetic and biometric data for identification. Special Categories of Personal Data can only be processed under strict conditions and such processing will usually, although not always, require the explicit consent of the data subject.

1. Introduction and Background

1.1 The Catholic Diocese of Portsmouth (the "Diocese") is a Data Controller and consequently must process all Personal Data (including Special Categories of Personal Data) about Data Subjects in accordance with the UK General Data Protection Regulation (the "UK GDPR") and any other relevant data protection legislation, domestic or otherwise, (as may be in force or repealed or replaced from time to time) (together the "Data Protection Rules"). After the UK left the European Union on 31 Dec 2020, the UK General Data Protection Regulation (UK GDPR) replicated the content of the previous EU GDPR regulations. For the avoidance of doubt, the Diocese remains the sole Data Controller, even where Processing is carried out by its curial offices, parishes, departments, and agencies.

1.2 The Diocese will collect, store, use and otherwise process Personal Data about the people with whom it interacts, who are the Data Subjects. This may include parishioners, volunteers, clergy, employees, contractors, suppliers and other third parties.

1.3 It is therefore of vital importance that any data, observations, or opinion written about any data subject is done so in an accurate and respectful way that if shared with the individual would not embarrass or support any litigation brought against the Diocese

1.4 The Diocese processes Personal Data so that it can comply with its statutory obligations and achieve its charitable objects of advancing and maintaining the Roman Catholic religion through the operation of its parishes and its other activities.

1.5 Every Data Subject has several rights in relation to how the Diocese processes their Personal Data. The Diocese is committed to ensuring that it processes Personal Data properly and securely in accordance with the Data Protection Rules, as such commitment constitutes good governance and is important for achieving and maintaining the trust and confidence of Data Subjects. Therefore, the Diocese will regularly review its policies and procedures to ensure that they are adequate and up to date every three years.

1.6 All Trustees, clergy, employees, and volunteers of the Diocese who are involved in the Processing of Personal Data held by the Diocese have a duty to protect the data that they process and must comply with this Policy. The Diocese will take any failure to comply with this Policy or the Data Protection Regulation very seriously. Any such failure may result in legal action being taken against the Diocese or the individual responsible.

2. The Data Protection Principles

2.1 The Diocese as the Data Controller is required to comply with the seven data protection principles set out in the UK GDPR, which provide that Personal Data must be:

a. Processed fairly, lawfully and in a transparent manner.
b. Collected for specified, explicit and legitimate purposes and not further processed for other purposes incompatible with those purposes.
c. Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
d. Accurate and, where necessary, kept up to date – every reasonable step must be taken to ensure that inaccurate personal data is erased or rectified without delay.
e. Kept in a form that permits identification of Data Subjects for no longer than is necessary for the purposes for which the personal data is processed; and
f. Processed in a way that ensures its security, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational security measures.
g. The accountability principle requires you to take responsibility for what you do with personal data and how you comply with the other principles. You must have appropriate measures and records in place to be able to demonstrate your compliance.

3. The Diocesan Data Protection Officer and Registration with the ICO

3.1 The Diocesan Trustees have overall responsibility for compliance with the Data Protection Rules. However, the diocesan Data Protection Officer (DPO) shall be responsible for ensuring day-to-day compliance with this Policy and the Data Protection Rules. The DPO will undergo training at least once every 12 months and the Diocese will provide the DPO with sufficient resources and support to carry out their responsibilities. The DPO's name and contact details can be found in section 15 of this Policy.

3.2 The Data Compliance Officer (DCO) is an employee in the Curia's Governance department, who deals with the day-to-day administration of diocesan data protection and liaises with the DPO. Contact details for the DCO can be found in section 15 of this Policy.

3.3 The Catholic Diocese of Portsmouth is the 'Controller' of all personal data that is processed by any Diocese member (trustee, clergy, employee, or volunteer). This

means that anyone who acts on behalf of the Diocese by processing personal data must act within the data protection regulations. All use of personal data is formal no matter who in the Diocese deals with it.

3.4 The Parish Priests have overall responsibility for ensuring our compliance with Data Protection legislation within their Parish.

3.5 They will ensure that:

a. the Diocesan Data Protection Policy is implemented and communicated effectively.
b. a data protection culture of continuous improvement is created, and progress monitored.
c. all data protection requirements are met.
d. parish Data Protection Representatives are appointed to provide data protection assistance.
e. there is regular communication and consultation with employees and volunteers on data protection issues.
f. employees and parish Data Protection Representatives are encouraged to complete Diocesan data protection training programmes.
g. Diocesan systems of work, risk assessment procedures and advice provided by the Diocesan DPO are implemented; and
h. data protection incidents are recorded, investigated, and reported via the Personal Data Breach Report form available on the website.

3.6 The Diocese is registered with the Information Commissioner's Office (the "ICO") as a Data Controller and will renew its registration annually as is required by law.

3.7 This Policy applies to all Personal Data processed by the Diocese in whatever format (e.g., paper, electronic, film) and regardless of how it is stored (e.g., electronically, or in filing cabinets if there is an ordered filing system in place). It also includes information that is in paper form but is intended to be put into electronic form, and to any recordings made such as telephone recordings and CCTV.

4. How the Diocese will Comply and Demonstrate Compliance

4.1 This Policy is intended to ensure that any Processing of Personal Data is in accordance with the Data Protection Rules and the data protection principles. The Diocese will therefore:

a. Ensure that, when personal information is collected, a data collection form including a short Privacy Notice is used (see Appendix B for templates) to

ensure the Data Subject is made aware of the Diocese's full Privacy Notice and informed of what data is being collected and under which lawful basis.

b. Be transparent and fair in processing Personal Data.

c. Take steps to ensure the accuracy of data at the point of collection and at regular intervals, thereafter, including advising Data Subjects of their right to ask for rectification of Personal Data held about them.

d. Securely dispose of inaccurate or out-of-date data, or data which is no longer required for the purpose(s) for which it was collected.

e. Share information with others only when it is lawful to do so and ensure that individuals are informed of the categories of recipient to whom data will or may be disclosed and the purposes of any such disclosures.

f. Ensure that additional safeguards (as required by the Data Protection Rules) are in place to protect Personal Data that is transferred outside of the UK (see Section 11).

g. Ensure that data is processed in line with the Data Subject's rights, which include the right to:

   i. request access to Personal Data held about them by the Diocese (including, in some cases, having it provided to them in a commonly used and machine-readable format).

   ii. have inaccurate Personal Data rectified.

   iii. have the processing of their Personal Data restricted in certain circumstances.

   iv. have Personal Data erased in certain specified situations (in essence where the continued processing of it does not comply with the Data Protection Rules).

   v. object to the processing of their Personal Data in certain circumstances such as for direct marketing purposes.

   vi. ask the Diocese to prevent Processing of Personal Data which is likely to cause unwarranted or substantial damage or distress to the Data Subject or any other individual; and

   vii. prevent, in some cases, decisions being made about them which are based solely on automated processing (i.e., without human intervention) and which produce significant or legal effects on them.

h. Ensure that all Trustees, Clergy, volunteers, and employees are aware of and understand the Diocese's data protection policies and procedures; and

i. Adopt a Data Retention Policy which sets out the periods for which different categories of Personal Data will be kept.

4.2 Through adherence to this Policy and related data protection policies, and through appropriate record-keeping, the Diocese will seek to demonstrate compliance with each of the data protection principles.

4.3 In addition, the Data Protection Rules require the Data Controller to carry out a Data Protection Impact Assessment (a "DPIA") prior to undertaking any Processing of Personal Data that is "likely to result in a high risk for the rights and freedoms" of individuals. DPIAs will therefore be considered where appropriate in relation to the implementation of any new projects, services or systems which could result in a high privacy risk to individuals. Please contact the DPO for guidance (see section 15 of this Policy).

5. Data Security & Responsibilities of Trustees, Clergy, Employees, and Volunteers

5.1 The Diocese must ensure that appropriate technical and organisational security measures are in place to prevent unauthorised or unlawful Processing, damage to, loss (accidental or otherwise), theft, or unauthorised disclosure of Personal Data (a "Data Breach"). All Trustees, Clergy, employees, and volunteers must ensure that:

a. The only individuals who have access to Personal Data and can process it are those who are authorised to do so.
b. Personal Data is stored only on the Diocese server (SharePoint and OneDrive) and not on individual PCs (unless they are encrypted), portable electronic devices or removable storage media.
c. Passwords are strong, kept confidential, are changed annually by users, are not shared between individuals, and are changed when a user of a shared mailbox leaves their role.
d. PCs are locked or logged off and paper documents are securely locked away when individuals are away from their desks.
e. Offices, desks and filing cabinets/cupboards are kept locked if they contain Personal Data of any kind, whether in digital or electronic format or on paper.
f. When destroying Personal Data, paper documents are securely shredded, and electronic data is securely deleted.
g. A record (e.g., spreadsheet log, see Appendix B for template) must be kept describing the type of personal data disposed of, date disposed of, method of disposal, and the reason for disposal (e.g., in line with Retention Schedule), and
h. Personal Data removed from an office is subject to appropriate security measures, including keeping paper files in a place where they are not visible or accessible by the public, using passwords/passcodes, and storing such devices securely (e.g., not left in the boot of a car overnight).

5.2 In the event that you become aware that there has been a Data Breach, you must report this immediately to the DCO at gdpr@portsmouthdiocese.org.uk using the Personal Data Breach Report form.

6. Privacy Notice

6.1 When any information is collected from an individual, they must be made aware of the Diocese full Privacy Notice, made available on the Diocese website or from the parish office. The Diocese full Privacy Notice provides information about what, why and how all personal data information in the Diocese is processed. You should make yourself aware of it.

6.2 In addition, every form that collects personal data must also include a Short Privacy notice that is specific to the use of data collected on that form.

7. Processing, Disclosure and Sharing of Information

7.1 The Diocese processes personal data for several different purposes, including:

Lawful Basis for Processing Personal Data	**Examples (not an exhaustive list)**
Where we have an individual's consent	Adding their contact details to a parishioner database or mailing list for specific purposes. Posting photographs of an individual on a diocesan website Providing information for the administration of a wedding
Where we have parental consent for an under-18-year-old	Consent for an under-18-year-old to attend a class, youth group, or go on a trip.
Where it is necessary for the performance of a contract to which an individual is party	Providing information to a photographer about photos required for a wedding Fulfilling a contract of employment

Where it is necessary for compliance with a legal obligation	Passing on information to the local authority Passing on tax information to HMRC
Where it is necessary to protect the vital interests of an individual	Passing on information to the Police where there is a risk of death or serious injury to that person or another individual Passing on information about an individual's serious health condition to the NHS or a health professional where there is a risk of death or serious injury to that person or another individual
Where it is necessary for performance of a task in the public interest	Updating and maintaining the register of marriages Carrying out certain safeguarding activities
Where is it necessary for the purposes of the legitimate interests pursued by the Diocese or a third party	Using baptism data to follow up with families for first communion Contact by a third-party company contracted to run a Diocese fundraising campaign

Lawful Basis for Processing of Special Categories of Data (e.g., ethnic origin, religious beliefs, health data etc) – additional safeguards are required	**Examples (not an exhaustive list)**
Where we have an individual's explicit consent	To cater for your dietary or medical needs at an event
Where it is necessary for compliance with a legal obligation	If the Diocese has received a court order to provide personal data
Where it is necessary to protect the vital interests of an individual	Passing on information to the Police where there is a risk of death or serious

	injury to that person or another individual Passing on information about an individual's serious health condition to the NHS or a health professional where there is a risk of death or serious injury to that person or another individual
Where it is carried out during the Diocese's legitimate activities by a not-for-profit body with religious aims, and the personal data will not be shared with any external party and will be kept securely in line with the data protection principles.	Using parishioners' health related data for pastoral visits Using parishioner or volunteer databases to assist with parish administration (e.g., rotas)
Where information has manifestly been made public	The religious beliefs of a member of the clergy are deemed to be manifestly public, but the religious beliefs of the laity are not and so it is sensitive information that requires explicit consent to share.
Where we are establishing, exercising, or defending legal claims	Legal advice will be sought in this instance
Where the processing is for reasons of substantial public interest	Where we are arranging insurance for a group of parishioners in advance of a pilgrimage
Where the processing is necessary for archiving historical records	Maintenance of parish records

8. Disclosing Personal Data

8.1 When receiving telephone or email enquiries, Clergy, employees, and volunteers should exercise caution before disclosing any Personal Data. The following steps should be followed:

a. Ensure the identity of the person making the enquiry is verified and check whether they are entitled to receive the requested information (i.e., has the person(s) the data is about given their consent to share; is the activity listed in our Privacy Notice).

b. Personal data collected by the Diocese (e.g., contact details) can be shared within the Diocese for legitimate Diocese activities that are listed in our Privacy Notice. However, explicit consent is required to share personal data with any party external to the Diocese.
c. If the person's identity cannot be verified, ask them to submit their request in writing so further checks can be made.

d. When providing files containing personal data, ensure it is sent by secure and appropriate means (e.g., using the Diocese secure email server and restricted access file links; sensitive data such as for vulnerable people, under-18s or financial data should also be password-encrypted, or in limited circumstances for paper files send by special delivery or hand delivery).
e. If a person requests access to their own personal data that the Diocese holds about them, please inform the DCO immediately, as there are specific criteria and deadlines for responding. They will be directed to the Subject Access Request (SAR) process on the Diocese website.
f. Personal Data must not be disclosed to any enquirer save and except in accordance with this policy and any statutory obligations of the Diocese; and
g. If there is any doubt, refer the request to the DCO for assistance (particularly where Special Categories of Personal Data are involved).

8.2 Please remember the personal data of under-18-year-old belongs to them and not their parents and so we cannot disclose personal data without the under-18-year old's consent unless another lawful basis applies. Children from approximately 12 years and older are entitled to make their own requests (where the Diocese is of the reasonable view that they have an appropriate understanding of the request). If you are unsure about whether to provide information about a child to a parent or guardian, please speak to the DCO before providing any information.

9 Data Processors

9.1 The Diocese may instruct another body or organisation to process Personal Data on its behalf as a Data Processor (e.g., a payroll provider, a third-party IT provider, delivery of parish newsletters). In such situations, the Diocese will share necessary information with the Data Processor but will remain responsible for compliance with the Data Protection Rules as the Data Controller.

9.2 Personal Data will only be transferred to a third-party Data Processor if the DPO is satisfied that the third party has in place adequate policies and procedures to ensure compliance with the Data Protection Rules. There should be a written contract in place between the Diocese and the Data Processor as well, which

includes provisions to ensure that the Data Processor complies with the requirements of the Data Protection Rules.

10 Third Party Requests

10.1 The Diocese may from time to time receive requests from third parties for access to documents containing Personal Data. The Diocese may disclose such documents to any third party where it is legally required or permitted to do so by law. Such third parties may include health professionals, the Police and other law enforcement agencies, HMRC, other regulators, immigration authorities, insurers, local authorities (e.g., Trading Standards) or Courts and Tribunals.

10.2 Anyone in receipt of any verbal or written request from any person for access to, or disclosure of, any Personal Data outside of normal Diocesan operations must immediately contact the DCO.

11 Transfers of Personal Data Outside of the UK

11.1 The Data Protection Rules require Data Controllers to put additional safeguards in place when transferring or accessing Personal Data outside of the UK. Additionally, such transfers or access can only take place on specific legal grounds. Save in respect of the Channel Islands, the Diocese does not store personal data outside of the UK. The UK has "adequacy regulations" which allows transfers of data to Guernsey and Jersey (see ICO website for more details).

11.2 Where any such personal data is stored outside of the UK then it is stored under conditions that are no less onerous than the requirements of the UK General Data Protection Regulation (UK GDPR) or any successor legislation. However, the Diocese may transfer Personal Data outside of the UK where requested by the Data Subject, based on the Data Subject's informed consent. This includes, but is not limited to, the situation where a Data Subject requires their marriage record to be sent to a non-UK country. Transfers may also take place where another legal ground in the Data Protection Rules is met.

12 Subject Access Requests (SARs)

12.1 Any Data Subject may exercise their rights as set out above (e.g., the right of access to the Personal Data which the Diocese holds about them, or the right to have Personal Data erased). Individuals can make SARs verbally or in writing, including via social media. We will request that SARs are submitted in writing and provide enough information to enable the Diocese to identify the Data Subject and to comply with the request. Requesters will be directed to the Subject Access Request (SAR) process on the Diocese website.

12.2 All Subject Access Requests will be dealt with by the DCO and the Governance and IT departments, in liaison with the DPO. Clergy, employees, or volunteers who receive a Subject Access Request must forward it to the DCO **immediately** gdpr@portsmouthdiocese.org.uk in order that such requests can be replied to within the strict deadlines set out in the Data Protection Rules (generally one month from the date of the request).

12.3 No fees will be charged for dealing with Subject Access Requests unless a request is manifestly unfounded, excessive, or repetitive. Fees may be charged to provide additional copies of information previously provided. Where the Diocese considers a request to be manifestly unfounded, excessive, or repetitive, the Diocese may lawfully refuse to respond and, if so, the DPO will inform the Data Subject of this in writing within the one-month period.

12.4 The Diocese may extend the time to respond to a SAR by up to an additional sixty days if for example technical or legal advice needs to be sought to respond and, if so, the DPO will inform the Data Subject of this in writing within the one-month period.

12.5 Following the response to the SAR, if the data subject is not happy with the result, they may contact the Diocese to instigate the level 2 process of the Diocese Complaints Procedure. The complainant may also escalate any concerns to the ICO.

13. Fundraising and Marketing

13.1 Any use of Personal Data for marketing (including fundraising) purposes must comply with the Data Protection Rules and the Privacy and Electronic Communications Regulations (the "PECR") (and any replacement legislation) which relate to marketing by electronic means.

13.2 Individuals have a right to object to their Personal Data being used for electronic marketing purposes. Individuals must be informed of their right to object when their data is collected. If an objection is received it must be logged on a 'do not send' list and no further marketing or fundraising communications will be sent to them. The PECR require that the Diocese has the prior consent of recipients in certain circumstances before it sends any unsolicited electronic messages for the purpose of fundraising, or other marketing activities (e.g., events).

13.3 Please note that the PECR 'soft opt-in' condition, that when purchasing goods or services a data subject may be added to a mailing list unless they opt out, does not apply to non-commercial promotions such as charity fundraising. See ICO website for more details.

13.4 Any use of Personal Data for fundraising or direct marketing purposes which is not in accordance with the requirements set out above must be approved, in advance, by the DPO.

14 Monitoring and Review

14.1 This policy will be reviewed at least every 3 years and may be subject to change with the approval of the Trustee Board.

15 Contacts

15.1 Any queries regarding this Policy should be addressed in the first instance to the Diocesan Compliance Officer at gdpr@portsmouthdiocese.org.uk St Edmund House, Bishop Crispian Way, Portsmouth, Hampshire, PO1 3QA or to the Diocesan Data Protection Officer who can be contacted at hello@dpocentre.com The DPO Centre Ltd, 50 Liverpool Street, London, EC2M 7PY. Tel 020 3797 1289. (Registered No: 10874595).

15.2 Complaints will be dealt with in accordance with the Diocesan Policy for Complaints (non-Safeguarding).

15.3 Further advice and information can be obtained from the Information Commissioner's Office (ICO) at www.ico.org.uk

15.4 Data Subjects have the right to lodge a complaint with a supervisory authority, which, for the purposes of the UK, is the Information Commissioner's Office (ICO): Contact us | ICO

16 Other Information Governance Policies

16.1 This Policy must be read in conjunction with:

a. Diocesan Full Privacy Notice (GOV-PRO-003-01)

b. Retention Schedule (GOV-FRM-002-01)

c. Subject Access Request (SAR) Guidelines (GOV-FRM-014-01)

d. Bring Your Own Device Policy

e. Data Breach Procedure (GOV-PRO-004-01)

f. Policy for Complaints (non-Safeguarding) (GOV-POL-002-01)

Appendix A Procedures

1. **GDPR Factsheet**
   GDPR Factsheet

2. **Retention Procedure**
   Retention Procedure

3. **Full Privacy Notice for the Portsmouth Roman Catholic Diocese**
   Full Privacy Notice

4. **Data Breach Procedure**
   Data Breach Procedure

5. **CCTV Procedure**
   CCTV Procedure

Appendix B Forms and Guidance notes

6. **Notes on forms involving personal data**
   Notes on Forms

7. **Parishioner registration example form template**
   Parishioner Registration Form

8. **Parishioner volunteer example form template**
   Volunteer Registration Form

9. **Short Privacy Notice example to adapt for other forms**
   Short Privacy Notice

10. **Record of disposal**
    Record of Disposal

11. **Reminder of personal data held - Adults**
    Personal Data Reminder

12. **GDPR: Asking for consent checklist**
    Consent checklist

13. **Personal Data Breach Report Form**
    Data Breach Form

14. **Subject Access Request (SAR) Guidelines**
    SAR Guidelines

15. **Subject Access Request (SAR) Form**
    SAR Form

16. **Subject Access Request (SAR) Record version**
    SAR Record Version

17. **Subject Access Request (SAR) Response**
    SAR Response

18. **Email footer template**
    Email Footer

19. **Data Privacy Impact Assessment (DPIA)**
    DPIA

20. **Filing guidance - brief**
    Filing guidance - brief

21. **Filing Guidance – detailed**
    Filing guidance - detailed

22. **Abbreviations**
    Abbreviations