GDPR

AN INTRODUCTION FOR PRIESTS, STAFF AND VOLUNTEERS OF THE DIOCESE OF PORTSMOUTH

Introduction

During the course of your parish activities you will collect, store, use and otherwise process personal information about the people with whom you interact. This may include information about parishioners, clergy, volunteers, employees, contractors, suppliers and other third parties.

In May 2018, the Data Protection Act will be replaced by new General Data Protection Regulation, a new legal framework with greater scope and much tougher punishments for those who fail to comply with the requirement in respect of security and handling of personal information.

The Diocese will make every effort to achieve best practice in relation to data protection and presents the following guidance to help all comply with the GDPR legislation, whether priest, employee or volunteer. For this we rely on your help.

A few terms to explain:

Personal Data:	Information about a living person which is capable of identifying that person
Special Categories of Personal Data:	Highly sensitive data such as a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition, sexuality (and includes genetic and biometric data).
Data Coordinator:	Your local data 'expert'. Your parish priest in the absence of a named volunteer.
Data Protection Officer DPO:	The representative for our Diocese who audits and advises us on GDPR Mark James mark@mojou.co.uk
Processing:	Anything done with/to personal data
Diocesan Compliance Officer	The in-house representative who will liaise with the DPO: GDPR@portsmouthdiocese.org.uk Tel: 02392825430

Collecting Personal Data

Data subjects (you and me) now have rights about their personal data which is held by the Diocese whether collected by priests, staff or volunteers.

You need to tell individuals (GDPR Footnote template) what they are doing with the information that you are collecting. It is important therefore for you to be aware whether you are collecting data that is personal to an individual and/or special category data. Only collect personal data if

it is for a legal or legitimate purpose and limit it to what you actually need. Know how long you need the data, how you are going to keep it up to date and how you are going to dispose of it, and when. Further information is listed in the Retention Policy.

Examples of legitimate or relevant reasons to collect data might be:

- ✓ to provide pastoral care for parishioners
- ✓ to administer parish records and registers
- ✓ to fundraise and promote the interests of the parish
- ✓ to manage employees and volunteers
- ✓ to maintain own accounts and records
- ✓ to enable the provision of a voluntary service for parishioners/the public
- ✓ to provide a sacramental program
- ✓ to operate a website
- ✓ to information parishioners of news, events and activities
- ✓ to process gift aid applications

How to Keep Personal Data Secure

For each data process, you need to record the names of the people who may have access and note how the information will be limited to those named people. Think about the following:

- ✓ Are you aware of how to use your own device for Parish or Diocesan activities?
- ✓ Do you have a clear desk policy at the end of the day?
- ✓ Are PCs locked or logged off and paper documents securely locked away when individuals are away from their desks?
- ✓ If any individual PCs, portable electronic device, or removable storage media are used to store personal data, are they encrypted?
- ✓ Are passwords and PINs kept confidential and changed regularly?
- ✓ Are computer screens positioned away from windows and gangways to prevent accidental disclosure of personal data?
- ✓ Are offices, desks and filing cabinets/cupboards kept locked if they hold personal data of any kind, whether on computer or on paper at the parish office or at home?
- ✓ When you remove personal data from an office, is it subject to appropriate security measures, including keeping paper files away from public visibility, the use of passwords/passcodes and encryption of portable electronic devices and secure storage (eg. never take paper together with a laptop, never leave in boot of a car)
- ✓ When destroying personal data, are paper documents securely shredded and is electronic data deleted securely?
- ✓ Do you keep back-ups of information that also need deleting?
- ✓ When you replace an electronic device, do you delete the hard drive correctly?

Processing Data

You may only process data, that is use or do anything with or to the data, if at least one of the following conditions apply:

- Consent is obtained
- Contract obligation

- Legal Obligation
- Vital interest of data subject
- Public Interest
- Legitimate Interests of Diocesan activity.

When you collect data from a person, you need to tell them why you are collecting it, what it will be used for and with whom it may be shared. It is not enough just being aware of the reasons yourself. Data subjects need to be informed and this is done through the Diocesan Privacy Notice and, when necessary, Consent Forms.

The Privacy Notice

The Privacy Notice needs to be referred to on any forms or explanations given for collecting data. This may include emails, letters, etc.

Wording for use is as follows:

Information provided on this form, together with all other personal data held about these individuals by the Parish and the Diocese of Portsmouth, is processed in accordance with the Diocese's Privacy Notice; or from the parish office.

Consent

Sometimes, and possibly when collecting special categories of personal data, consent is also required; the Privacy Notice will cover only some reasons for collecting data. The following are examples where consent forms may be required. Consent forms must be kept and recorded as evidence that the data was collected legally:

- Fundraising and marketing
- Details of parishioners kept for a parish directory
- Social media
- Photographs

If in doubt seek advice from your Data Coordinator or Diocese
GDPR@portsmouthdiocese.org.uk

Further Processing of Data

If you or the Diocese wishes to use personal data for a new purpose, not covered by the Privacy Notice issued at the time of data collection, a new notice will need to be provided with an explanation and possibly a new consent form. Please refer to your Data Coordinator about Privacy by Design/Protection Impact Assessment before proceeding.

Subject Access Requests (SARS)

An individual may submit a request asking for the information you hold on them; they may wish to check accuracy, or where it came from. This is known as a Subject Access Request whether or not they mention that it is a Subject Access Request, or refer to the GDPR.

Dealing with SARs is complicated and **urgent** because the GDPR stipulates a strict timetable of a **month** within which these requests must be responded to. Notify your Data Coordinator or Diocesan Data Compliance Officer immediately and the parish priest.

Data Breach

A personal data breach is one that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.

Don't let your parish be the one that suffers a data breach. Think about the difference between a security incident and a data breach. If for example, a lap top is left on a train containing personal data but no one accessed that data (eg. Encrypted data) then it is a security incident.

However, if someone found and used the data, that is a data breach and the Diocese is legally obliged to report it to the ICO on your behalf within **72 hours** of you finding out. If you are aware of either a security incident or data breach, contact the Diocesan Data Compliance Officer, and your priest or parish local data coordinator immediately. The Diocese does and will need to act **quickly and legally** to limit the effect of the breach and avoid severe fines and penalties.

Compliance

Your Data Coordinator will contact you regularly and expect you to be able to show where you keep personal data, how you have kept to the GDPR and whether you have received training. Please therefore keep evidence of all your data transactions and training. Your parish Data Coordinator will explain that your parish completes an annual audit of all data held and they will rely on your compliance.

The Diocesan Operating Policy for Data Protection and related GDPR policies can be found the Diocesan website at www.portsmouthdiocese.org.uk/gdpr or via your Parish office. In addition training will be offered regularly and you are encouraged to attend. Please make contact with your parish Data coordinator and make them aware of your role, and the data that you are collecting, storing or using.