Diocese of Middlesbrough
Lourdes Pilgrimage

Data Protection Management Procedures

Name of originator/author:	Keith Tillotson
Date issued:	May 2018
Date Reviewed:	May 2026
Date next review due:	May 2028

Introduction

The Diocese of Middlesbrough Lourdes Pilgrimage will ensure that all Personal Confidential Data (PCD) and sensitive information obtained about its pilgrims is effectively managed and that appropriate policies, procedures, management accountability and structures provide a robust Information Governance (IG) framework.

This policy adheres to the requirements stated in the EU General Data Protection Regulation (GDPR) implemented in May 2018.

Due to the nature of the organisation this policy applies to Medical Records obtained for or created in pursuance of managing the health and safety of all actual and potential pilgrims relating to our pilgrimage to Lourdes each year and can encompasses all categories of pilgrim including helpers and clinical volunteers, not solely those travelling as supported pilgrims.

Scope

This policy guides the use of personal and sensitive information for the preparation and management of the pilgrimage both in England and while in Lourdes.

Information takes many forms, including data stored in databases, on computers (desktop, laptop or tablet); transmitted across networks; written on paper; sent by fax or email; stored on portable media; or spoken in conversations. This includes, but is not limited to all:

• information processed by the Pilgrimage in pursuit of all its pilgrimage activities.

• information processing facilities used in support of the Trust's pilgrimage activities to

store (electronically or physically), process and transmit information.

Technology moves quickly. To this end, the spirit of this policy applies to any emergent technology that will be used to support future pilgrimage administration. Future updates of the policy will be amended to consider any future changes of the GDPR and other initiatives.

Responsibilities

The Pilgrimage Director

The Pilgrimage Director has overall day-to-day responsibility for all aspects of the Lourdes Pilgrimage activities, and reports to the Bishop of Middlesbrough as their direct line manager.

The Pilgrimage Director incorporates the role of Senior Information Risk Owner (SIRO). In practical terms they are accountable for, and report to the Bishop and DPO on, issues of information risk within the Pilgrimage.

To this end, they must foster a culture for protecting and appropriate use of data; provide a focal point for managing information-related risks and incidents; and be concerned with the appropriate management of all information assets.

The Chief Medical Officer (CMO)

The Chief Medical Officer takes responsibility for all clinical decisions made prior to and during the Pilgrimage to Lourdes.

They are supported by a substantial team of clinicians who co-ordinate all medical support for the pilgrimage, supported by the clinical data supplied by each pilgrim, which is available to them in written and/or digital form.

They have a responsibility to ensure that all clinical volunteers are aware of and discharge their responsibilities for IG and confidentiality.

Pilgrimage Administration Volunteers

Pilgrimage administration volunteers are responsible for collating all information received from pilgrims applying to join the pilgrimage to Lourdes, so that it is available for the CMO when required. It is also their responsibility to ensure that all of the appropriate clinical data is stored effectively, and managed for the appropriate time in accordance with the Pilgrimage archive policy for each and every item of data captured.

The Pilgrimage Heads of Department are responsible for ensuring appropriate IG guidelines are followed within their area of responsibility.

Volunteer Group Leaders, Co-ordinators & Helpers

Volunteer group leaders and co-ordinators have a responsibility, as guided by the Pilgrimage, to brief all those in their group regarding appropriate use and disclosure of information on the pilgrimage Formation Day and by reinforcing this policy throughout the pilgrimage in Lourdes.

Volunteer group helpers (Hospitalité) have a responsibility to be aware of and abide by the key aspects of this policy and to share any concerns with their Team Leader who in turn will share this with their respective Head of Department.

Training and Awareness

All volunteers will receive an update briefing on best practice at the annual pilgrimage Formation Day.

Definitions

There are several key concepts that need to be understood to ensure an effective Governance is created and maintained.

> *Information Governance allows organisations and individuals to ensure that personal information is handled legally, securely, efficiently and effectively, in order to deliver the best possible care. It additionally enables organisations to put in place procedures and processes for their corporate information that support the efficient location and retrieval of corporate records where and when needed, in particular to meet requests for information and assist compliance with Corporate Governance Standards.*

More generally, Information Security is understood as the preservation of confidentiality, accuracy and availability of information, while other properties, such as authenticity, accountability, non-repudiation, and reliability are also involved.

Personal Confidential Data is understood as personal information about identified or identifiable individuals, which should be kept private. This includes the GDPR definition of personal data, but is adapted to include people who are deceased, as we as the living. Confidentiality is also taken to include 'sensitive' information as defined in the GDPR.

The GDPR definition of Personal data is that it relates to a living individual who can be identified from the data or from the data and other information which may come into the possession of the data controller, and includes expressions of opinion about them.

Sensitive personal, data under the GDPR, is personal data consisting of information as to an individual's racial/ethnic origin, political opinion, religious or other beliefs, membership of a trade union, physical or mental health, sexual orientation or activity, commissioning or alleged commission of an offence, and/or proceedings for any offence committed or alleged to have been committed by them.

Fundamental Principles

Central to an effective Data Protection framework are the application of three sets of interrelated guidance. It is the policy of Trust that these will be adopted in the management of its activities:

The General Data Protection Rules

The principles of the GDPR are, in summary:

- You must have a valid lawful basis in order to process personal data.
- There are six available lawful bases for processing. No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on your purpose and relationship with the individual.
- Most lawful bases require that processing is 'necessary' for a specific purpose. If you can reasonably achieve the same purpose without the processing, you won't have a lawful basis.
- You must determine your lawful basis before you begin processing, and you should document it. We have an interactive tool to help you.
- Take care to get it right first time - you should not swap to a different lawful basis at a later date without good reason. In particular, you cannot usually swap from consent to a different basis.
- Your privacy notice should include your lawful basis for processing as well as the purposes of the processing.
- If your purposes change, you may be able to continue processing under the original lawful basis if your new purpose is compatible with your initial purpose (unless your original lawful basis was consent).
- If you are processing special category data you need to identify both a lawful basis for general processing and an additional condition for processing this type of data.
- If you are processing criminal conviction data or data about offences you need to identify both a lawful basis for general processing and an additional condition for processing this type of data.

Ensuring an Effective Information Governance Framework

There are several processes that the Pilgrimage Committee employs, or is in the process of implementing, to ensure an effective and legal IG framework.

These are:

Data Quality: Ensuring that all information that is held about pilgrims and used to make decisions about them is as accurate as possible, and triangulated with other sources to maintain that accuracy on an ongoing basis.

Privacy Impact Assessment: Ensuring that a Privacy Impact Assessment (PIA), essentially a Data Protection/IG risk assessment, is undertaken in line with guidance from the Information Commissioner's Office, when new and/or significantly enhanced processes and/or systems are introduced.

Information Asset Management: This takes two forms, first ensuring the Pilgrimage Committee is aware of the Information Assets it holds (both paper and electronic), and basic information about them, such as who has access to the data, how that access is granted etc. This information is held in an Information Asset Register. Secondly, a process of Data Flow Mapping identifies and logs where data from these systems is sent to/received from. Both can assist in the assessment of Risks and/or support the recovery of information/assessment of damage if there is a breach.

Contracting arrangements: Maintaining a robust schedule of organisations with which the Pilgrimage Committee shares PCD about pilgrims (and volunteers), and annually reviewing them to ensure that they have effective IG clauses included, specifically around appropriate management of PCD under the DPA and reporting back of incidents to the Pilgrimage Committee, should they occur.

Information Security: Ensuring a strict application of Information Security principles both in the Lourdes Office in the UK and while in Lourdes, so as to maintain the confidentiality, integrity and availability of pilgrims (and volunteers) information.

Medical Records Retention and Destruction

Policy regarding retention and destruction of pilgrimage held Medical Records is based on our understanding of the principles of GDPR.

- Adult physical health records must be kept for eight years after their last interaction with the organisation.
- Paediatric physical health records must be kept until their 25th birthday or if the pilgrim was 17 at the conclusion of their interaction, until their 26th birthday.
- Mental health records must be kept for 20 years or 8 years after the pilgrim has passed away.

If there is a conflict in between the retention periods due to two or more of the above rules potentially applying, records are kept for the longest period.

Best practice suggests that it advisable for a clinician or suitably trained administrator to review any records prior to their destruction to prevent any inappropriate retention or destruction. Once the need for destruction is agreed, records must be destroyed under confidential conditions, such as using a cross-cutting shredder or an accredited confidential disposal company.

The DPO or the Chief Medical Officer or a trained administrator should retain a signed document confirming which documents were agreed for destruction.

This is undertaken en-masse on an annual basis shortly following each pilgrimage, in the latter part of the calendar year.