



# Data Protection Impact Assessment (DPIA) Procedure

Document date: February 2023



*Together, pursuing life in all its fullness*

<b>Version</b>	<b>Date</b>	<b>Author</b>	<b>Changes</b>
v1.0	February 2020	P. Blenkinsopp	Initial Issue
V1.1	February 2023	P. Blenkinsopp	Review and new clause 3.4

<b>Review frequency</b>	3 years
<b>Review date</b>	February 2026
<b>Ratified by</b>	Trust Leadership Team
<b>Date of ratification</b>	6 <sup>th</sup> February 2023
<b>Lead/owner</b>	Head of Operations and Compliance
<b>Target audience</b>	All Staff
<b>Document reference</b>	POL-DP03

The electronic version is the definitive version of this document.

## Contents

1	Introduction	4
2	Scope	4
3	When is a DPIA Required	5
4	Performing a Data Protection Impact Assessment	6
5	Conclusion	7
6	Changes to this Procedure	7

## 1 Introduction

- 1.1 This internal Data Protection Impact Assessment (**DPIA**) procedure (hereinafter “the Procedure”) aims to provide evidence that Diocese of Coventry Multi Academy Trust (“the Trust”) is fully committed to protecting personal data that is collected and processed on behalf of its workforce, pupils and parents. It also aims to provide detailed guidance on the measures that the Trust has adopted to ensure that personal data is collected, stored and processed in accordance with the rules laid down by data protection laws.
- 1.2 Under data protection laws, certain listed types of processing or any other processing that involve the processing of personal data that is likely to result in a high risk to individuals’ interests are subject to a DPIA. This is a key element of the new focus on accountability, data protection by design and is the cornerstone of a risk-based approach to compliance.
- 1.3 The Trust therefore asks you to carefully read this Procedure as it sets out the Trust’s our approach to DPIA’s and explains how to use the associated templates to ensure legal obligations are met.

1.4 Below, some terms which are frequently used in this Procedure are listed:

- **Personal data:** data which relates to a living individual who can be identified, directly or indirectly, from those data; or who can be identified from those data together with other information which could come in the possession of the Trust or of a third party.

This includes, for instance: contact details stored in email contacts, CVs obtained in relation to job candidates, market research details, customer or user data, digital photos, employee data (e.g. bank account number for salary payment) etc.

In essence, this covers any information identifying a living individual.

- **The data subject:** the individual whose personal data is being processed.
- **Processing:** in relation to personal data, processing means any activity that can be performed with such data, e.g. collection, use, organization, storage, review, adaptation, alteration, transfer or destruction of data.
- **Controller:** the legal entity, i.e. usually a Trust itself or its customers and not a specific employee of that Trust, which determines the means and purpose of the processing of the personal data. The Trust is the controller if it alone determines the means and purpose of the processing.
- **Processor:** a legal entity that processes personal data on behalf of a data controller. As an example, a cloud service provider or a provider which in some other way, e.g. in accordance with a customer agreement, has access to personal data could be a data processor.
- **National law:** the laws and regulations governed by and interpreted by the courts of England and Wales in accordance with English law.

## 2 Scope

- 2.1 The DPIA process comprises two parts, an initial screening that must be carried out for all new projects that intend to process personal data. This

screening is a simple exercise that identifies those projects that pose a high risk to individuals and will require a full DPIA. When a DPIA is required, the Trust must be able to demonstrate that it has considered both the likelihood and the severity of any impact on individuals taking into account the specific nature, scope, context and purposes of the processing.

2.2 The DPIA procedure will help to screen projects for factors which point to the potential for a widespread impact on individuals.

### 3 **When is a DPIA Required**

3.1 This Procedure applies to all projects where the Processing of Personal Data is “likely to result in a high risk to the interests of individuals”.

3.2 In particular, data protection laws state that a DPIA must be performed where the proposed processing activity involves:

- a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
- processing of special category or criminal offence data on a large scale; or
- systematically monitoring publicly accessible places on a large scale.

3.3 In addition, the Information Commissioner’s Office (**ICO**) requires organisations to perform a DPIA when they plan to:

- use new technologies;
- use profiling or special category data to decide on access to services;
- profile individuals on a large scale;
- process biometric data;
- process genetic data;
- match data or combine datasets from different sources;
- collect personal data from a source other than the individual without providing them with a privacy notice;
- track individuals’ location or behaviour;
- profile children or target services at them; or
- process data that might endanger the individuals’ physical health or safety in the event of a security breach.

3.4 A DPIA will be required whenever the processing involves the sharing of Pupil personal data with a third party.

- 3.5 A DPIA should also be considered for any other processing which is large scale, involves profiling or monitoring, decides on access to services or opportunities, or involves sensitive data or vulnerable individuals.
- 3.6 The screening questions template should be completed by the project manager, programme manager or GDPR owner at the start of any project that will require the processing of personal data. The screening questions will allow the project to assess its processing activity or type of personal data used against the screening questions set out in the template.
- 3.7 Once the screening questions have been completed, a score will be calculated and displayed at the bottom of the template. A score higher than 2 will require a DPIA to be performed.

#### 4 **Performing a Data Protection Impact Assessment**

- 4.1 If the initial screening indicates that a DPIA will be required then it is the responsibility of the project lead to complete this process at the start of the project planning activities. The DPIA Full Assessment template should be used to both facilitate the process and document the results.
- 4.2 Completion of the DPIA may require the involvement of a number of people including the project team, business stakeholders, IT, data protection, security, etc. It is the responsibility of the project lead to identify the necessary participants and ensure that they participate in the process.
- 4.3 The participants will need to work together to complete all sections of the DPIA with as much detail as possible in order to identify any risks.
- 4.4 The DPIA template is split into a number of tabs focussed on specific requirements of the GDPR.

##### **Scope**

This section is used to describe the scope of the project and its use of personal data. It requires details on the types of personal data used, what activities will be performed against this data, whether any sensitive (special categories) data is required, details on the formats and volumes of the data, who has access to it, whether the data is transferred outside of the EEA.

##### **Principles**

Requires the team to assess the projects use of data against the six core principles of the GDPR. These are that data is collected in lawful, fair and transparent manner, is only used for specified purposes, is only collected if required for the stated processing, is accurate and kept up to date, is only retained for as long as necessary and is kept in a way that protects integrity and confidentiality.

##### **Data Protection**

What technical and organisational measures will be put in place to protect the data when the project is live. This section requires details of all the measures that are planned to be introduced to protect the data. If multiple systems and

processes are planned then they should be split out and numbered, i.e., System/Process # 1; System/Process # 2, etc.

### **Rights of the Data Subject**

This section should be used to ensure that the rights of the data subjects have been met through privacy notices and that the system will enable the Trust to respond to any data subject who exercises their rights within the statutory prescribed timescales.

### **Risks**

The team should use the information gathered in the tabs 1 to 4 to identify any risks to the interests of individuals and to the business. Whilst these risks are normally focussed on data privacy, the project team should also consider other effects on the data subject depending on the nature of the proposed processing. Any risks identified should be recorded with as much detail as possible. The risks are then scored against likelihood (1= unlikely, 3 = likely) and impact (1 = low. 3 = high) which will produce a calculated risk score. This risk score is then used to classify the risk as shown below:

Risk Level	From	To	GDPR Assessment	Description of risk level
High	6	9	High risk	<i>the risk exceeds the organisation's risk appetite</i>
Medium	3	5	Unacceptable risk	<i>the risk could exceed the risk appetite under some conditions</i>
Low	1	2	Acceptable risk	<i>the risk is within acceptable bounds</i>
Zero	0	0	No risk	

Any risk calculated as medium or high will need to be mitigated before the project will be allowed to proceed.

The residual risk columns in the assessment should be completed by the project team and the likelihood and impact re-assessed to determine if the mitigation has successfully reduced the risk to an acceptable level. The risk treatment owner should also be documented for future reference.

Finally, the any risk treatment should be checked to ensure that the privacy principles have not been broken before the risk is approved by the compliance team.

## **5 Conclusion**

- 5.1 Performing impact assessments is both a legal requirement and also a fundamental part of delivering a successful project that processes personal data. The process of identifying the risks to both individuals and to our business is critical to our objectives of providing appropriate levels of protection of people's personal data and meeting their expectations of us in managing and controlling risks.

## **6 Changes to this Procedure**

This procedure is subject to change at any time.