GDPR – Data Protection Impact Assessment (DPIA) Policy & Procedure

October 2020

Our Lady of Lourdes Catholic Multi-Academy Trust - Company Number: 7743523
Registered Office: 1st Floor, Loxley House, Riverside Business Park, Tottle Road, Nottingham NG2 1RT

What is a Privacy Impact Assessment?

A Data Protection Impact Assessment ("DPIA") is a process that assists organisations in identifying and minimising the privacy risks of new projects or policies. Projects of all sizes could impact on personal data. The DPIA will help to ensure that potential problems are identified at an early stage, when addressing them will often be simpler and less costly.

Conducting a DPIA should benefit the [Trust/School] by producing better policies and systems, and improving the relationship with individuals.

Why should I carry out a DPIA?

Carrying out an effective DPIA should benefit the people affected by a project and also the organisation carrying out the project. Whilst not a legal requirement, it is often the most effective way to demonstrate to the Information Commissioner's Officer how personal data processing complies with data protection legislation. A project which has been subject to a DPIA should be less privacy intrusive and therefore less likely to affect individuals in a negative way. A DPIA should improve transparency and make it easier for individuals to understand how and why their information is being used.

When should I carry out a DPIA?

The core principles of DPIA can be applied to any project that involves the use of personal data, or to any other activity that could have an impact on the privacy of individuals.

Answering the screening questions in Section 1 of this document should help you identify the need for a DPIA at an early stage of your project, which can then be built into your project management or other business process.

Date Issued	October 2020
Date of Review	October 2023
Reviewer	Karen Rich / OLoL Trust
Author	Browne Jacobson template – edited by Karen Rich

Data Protection Impact Assessment (DPIA) for new Projects or Systems

General Details

Project Title	
Project Lead	
Contact Details	
DPO	
Contact Details	
Date DPIA Completed	

General Project Description
Explain what the project aims to achieve, what the benefits will be to the organisation, to individuals and to other parties:

Will the project/system involve the processing of personal data or special category (sensitive) personal data?
YES / NO

If '**No**', please sign and forward the DPIA to the IT Security Manager, Head of Programme Office and Director of IT for their awareness and stored by the DPO for accountability purposes.

If '**Yes**', please complete the sections below:

1. Systematic Description of the Envisaged Processing Operations

1.1 Create a Data Flow Diagram and attach it as Annex 1 to this DPIA.

1.2 Identify the data subjects:

1.3 What personal data will be processed?

1.4 What special category (sensitive) data or criminal convictions data will be processed?

1.5 What are the purposes and lawful grounds for processing the personal data identified above?

	Personal Data	Purpose	Lawful basis
1			
2			
3			
4			
5			

1.6 Describe the nature, scope and context of the processing, including a functional description of the processing operations:

1.7 Describe the assets on which the personal data relies (hardware, software, people, paper, networks, transmission channels)

1.8 Set out the periods for retention of the personal data:

1.9 Set out details of any data sharing with third parties, including sub-processors:

1.10 Set out details of any data sharing outside the EEA or with any international organisations:

2. Necessity and Proportionality Assessment

2.1 If legitimate interest is identified as the lawful basis, set out details below:

a) Identify the legitimate interest b) Explain why processing is necessary for the identified legitimate interest c) Balance the legitimate interest against the rights and freedoms of the data subjects

2.2 Identify any personal data processed in a manner which is not necessary for the identified purpose:

3. Assessment of Risks to the Rights and Freedoms of the Data Subjects

Consider and describe the risks to the rights and freedoms of the data subjects in the following areas:

3.1 Lawfulness of processing

3.2 Fairness and transparency of processing

3.3 Data minimisation

3.4 Maintaining accurate and up to date data

3.5 Ability for data subjects to opt out or object to processing

3.6 Ability to respond to subject access requests

3.7 Rights of the data subjects

3.8 Transfers to third parties

3.9 Transfers outside the EEA or to international organisations

3.10 Retention and deletion

3.11 Data security

3.12 Further risks

4. Measures Envisaged to Address the Risks

4.1 Complete the following table using the risks identified above:

	Risk	Controls to be implemented	Proposed Mitigation
1			
2			
3			
4			
5			

5. Compliance with Guidance/Codes of Conduct

5.1 Identify any applicable guidance and/or codes of conduct issued by the Government, the ICO, the Commission or any relevant association or body:

5.2 Where applicable, set out details of compliance with any relevant guidance and/or code of conduct:

6. Involvement of Data Subjects

6.1 Where appropriate, seek the views of the data subjects or their representatives on the intended processing and set out the findings below:

6.2 If the views of the data subjects have not been sought, set out the rationale below, with reference to any commercial or public interests and the security of processing operations:

7. DPIA Review

7.1 Identify any planned changes to the project or system and set a date to review this DPIA:

7.2 This DPIA will be reviewed to assess if processing is performed in accordance with this DPIA on: [INSERT DATE]

8. Approval

This project was assessed and its Data Protection Impact Assessment approved by:

DPO: **Date:**

Headteacher: **Date:**

Annex 1 – Project Lead: Please attach Data Flow Diagram