Bishop Wilkinson
Catholic Education Trust
Through Christ, in Partnership

Data Protection Impact Assessment (DPIA) Process

Signed by the Chair	
Date Approved by Trust	**15 July 22**
Statutory Policy	**No**
Required on Website	**No**
Review Period	**Annual**
Next Review Date	**July 2023**
Reviewed by	**DPO**

1. Revision History

The below table provides the revision history for this document. Each revision has an associated date, issue number, and description of the changes and/or content. The document revisions appear in descending order, with the most-recent iteration appearing first in the table.

Date	Version	Description	Author
18/05/2021	0.a	Initial Draft	Karen Latimer Data2Action
09/07/2021	0.b	Final Version	As above
15/07/2022	0.c	1st Review no changes	As above

2. Document Approval

Document Name	Data Protection Impact Assessment Process
Publication Date	July 22
Prepared by	Karen Latimer, Data2Action
Approval (Name & Organization)	BWCET Directors

3. Introduction

This document sets out guidelines relating to the necessity for and the completion of a Data Protection Impact Assessment (DPIA).

The Bishop Wilkinson Catholic Education Trust (the Trust) holds large amounts of personal and sensitive data and is responsible for safeguarding that data and is legally bound under the UK GDPR and Data Protection Act 2018 to ensure the security and confidentiality of all personal information processed. These responsibilities also extend to other organisations working on behalf of the Trust.

This document is for information and use by all employees of the Trust and associated schools, including any associates, contractors or agency staff and third-party processors.

Associated documents: Bishop Wilkinson Catholic Education Trust Data Protection Impact Assessment Template (Appendix A)

4. Overview of a Data Protection Impact Assessment

A Data Protection Impact Assessment (DPIA) is a process to help identify and minimise the data protection risks of any change initiative. You must complete a DPIA for any processing that involves the processing of personal data that is likely to result in a high risk to individuals. It is also good practice however to do a DPIA for any change initiative which requires the processing of personal data, irrespective of potential risk.

The UK GDPR highlights especially processing that uses new technologies such as Artificial Intelligence or Robotic Process Automation. Examples of where a DPIA is required are when deploying a new learning platform for use by pupils (for example, Class DoJo, Microsoft Teams, Google Classroom), implementing a new process that includes the processing of pupil (for example, CPOMS, SMID) and/ or staff data (for example, payroll).

When undertaking a DPIA the following criteria should be considered initially:

The purpose of processing:

- Why do you want to process the personal data?
- Is there any legitimate interest for processing?
- What will the result of the processing be?
- What will you achieve with the processing?

The context of processing:

- What is the source of the data which will be processed?
- How is your relationship with data subjects?

The nature of the processing:

- Who will have access to the data?
- Who will you share the data with?
- How is the data collected and stored?
- What are the defined retention periods for the data?
- What security measures have been taken to protect the data?
- How will you use the data?

The scope of processing:

- Required duration of the processing?
- Sensitivity of the personal data?
- Frequency and extent of the processing?
- The number of data subjects whose personal data will be involved in the processing.

5. The Data Protection Impact Assessment

The Data Protection Impact Assessment template (Appendix A) should be used to collate the following information after initial assessment:

- A systematic description of the processing operations undertaken (or proposed to be undertaken) including automated processing, processing on a large scale of special-category data or monitoring of a public accessible are on a large scale for example CCTV surveillance.
- Purposes of the processing, including if applicable, the legitimate interest pursued.
- Assessment of the necessity and proportionality of the processing operations in relation to the purposes.
- Assessment of the risks to the rights and freedoms of data subjects.
- Measures which could be implemented to address any risks including safeguards, security measures, mechanisms to be used to ensure the protection of personal data.

6. Identifying the Risks

When conducting the DPIA consideration should be given regarding any potential impact on individual data subjects. The aim is to identify any harm or damage your processing may cause whether physical, emotional or material, pay attention to assess whether processing could contribute to any of the following:

- Inability to exercise rights for example privacy rights
- Loss of control over the use of personal data
- Discrimination
- Identity theft or fraud

- Financial loss
- Reputational damage
- Physical harm
- Loss of confidentiality
- Reidentification of any anonymised data
- Economic or social disadvantage.

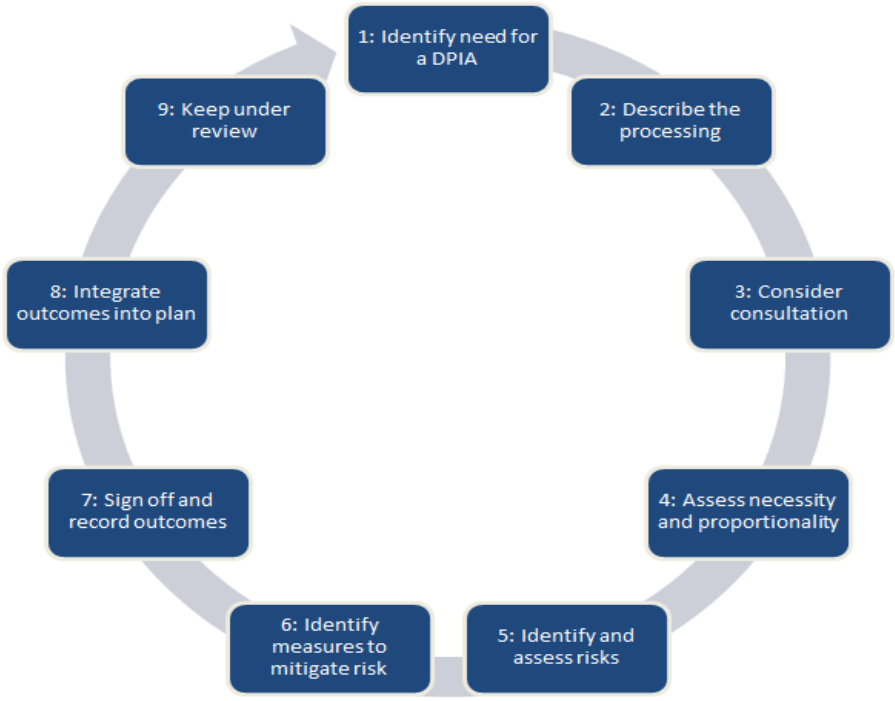
7. Possible Mitigating Actions

When you have identified any risks, you can then determine and consider any mitigating actions which could be implemented to reduce those potential risks for example:

- Deciding not to collect certain types of data
- Limiting the scope of processing
- Reducing the length of data retention periods
- Additional security measures
- Creating internal processes to avoid risks
- Anonymising data where possible
- Enforcing Data Sharing Agreements where necessary
- Making appropriate changes to Privacy Notices.

8. New Projects

A DPIA should begin early in the life of a project, before you start processing, and run alongside the planning and development process. It should include the below steps:



9. DPIA Approval

Following the completion of a Data Protection Impact Assessment the template should be issued to the Trust Data Protection Officer, Sarah Burns at the following email gdpr@bwcet.com

Approval must be gained prior to utilising the considered system or application referenced within the DPIA template. Any highlighted risks must be considered, with all applicable criteria demonstrated within an acceptable level.

10.When to Consult the Supervisory Authority

If a DPIA has been undertaken and it concludes even after all mitigation of risks have been enforced there will still be a high risk to the rights and freedoms of data subjects by processing, you must contact the supervisory authority should be contacted for further advice and guidance. This will be carried out with the support of the Trusts DPO.

The Information Commissioners Office (ICO) is the supervisory authority in the UK.

ICO contact details:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Helpline number: 0303 123 1113

Supporting Documentation

- Appendix A – DPIA Assessment