Academies Trust

8th Floor, Angel Square,
Manchester, M60 0AG

Data Protection Impact Assessment (DPIA) Guidance

Appendix 3 of the Data Protection Policy

Approved by the Trust Board on 2 October 2025

Applicable from 3 October 2025

Last Reviewed:	August 2025 (in preparation to seek approval in October 2025)
Reviewed by:	Tammy Pyszky, Head of Data Protection
Next Review Date:	October 2026
Version Changes:	Amendments to the process to include the role of the data protection ambassador. Addition of the need to consult regional directors and/or the audit and risk committee when necessary.

	Addition of the use of AI requiring a DPIA.

This document will be reviewed annually, or more frequently when significant changes are made to the law.

Contents

Appendix 3: Data Protection Impact Assessment Guidance

A3.1 Introduction

A Data Protection Impact Assessment (DPIA) is a tool to help us identify how to comply with our data protection obligations and protect individuals' rights.

An effective DPIA, carried out in the earliest planning stages of a project or change to policy, will allow us to identify and fix problems early on, reducing the associated costs, risks, and damage to reputation which might otherwise occur.

Step by step guidance and the necessary templates are available via the data protection ambassadors' toolkit, or from the Head of Data Protection.

DPIAs should be drawn up with the assistance of the Head of Data Protection or a Data Protection Ambassador, who will have the expertise needed to fully consider the issues, but the responsibility for ensuring a DPIA is undertaken lies with the staff member responsible for the project or policy.

A3.2 What is a Data Protection Impact Assessment (DPIA)?

A DPIA is a process which helps an organisation to identify and reduce the privacy risks of any project which involves personal data. To be effective a DPIA should be used throughout the development and implementation of the project.

A DPIA will enable the Trust or any of its academies to systematically and thoroughly analyse how a particular project or system will affect the privacy of the individuals involved, as well as provide evidence of investigation into the suitability of any third parties who will be given access to data in the project.

A3.3 When will a DPIA be appropriate?

DPIAs should be considered for all new projects, at the earliest stages, to allow greater scope for influencing how the project will be implemented. A DPIA can also be useful when planning changes to an existing system.

The Trust or any of its academies must carry out a DPIA for processing that is likely to result in a "high risk to individuals" (Article 35(1) UK GDPR). When considering whether the processing is likely to result in high risk, the following Information Commissioner's Office (ICO) Guidance should be considered:
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

This lists types of data processing that are likely to result in high risk. The most relevant to schools relate to:

- the processing of vulnerable data subjects (children);
- the processing of sensitive data or data of a highly personal nature;
- monitoring of people's online or offline behaviour;
- the use of innovative technologies (i.e. Artificial Intelligence)

Because so many activities in schools include the processing of children's data including sensitive data, it is likely that most projects in schools will require a DPIA to be carried out.

Prior to implementation, use of AI tools will be assessed to consider if a DPIA is required to determine whether their use is proportionate and fair. The DPIA will assess the benefits against the risks to the rights and freedoms to individuals and/or whether it is possible to put safeguards in place.

Conducting a DPIA does not have to be complex or time consuming but there must be a level of rigour in proportion to the potential privacy risks.

A3.4 The Benefits of a DPIA

Consistent use of DPIAs will increase the awareness of privacy and data protection issues within the Trust and its academies and ensure that all relevant staff involved in designing projects think about privacy at its earliest stages.

Examples of where a DPIA would be appropriate:

- Purchasing/implementing a new IT system for storing and accessing personal data;
- A proposal to identify people in a particular group or demographic and take action in relation to the group;
- Using existing data for a new and unexpected or more intrusive purpose;
- A new database which consolidates information held by separate parts of the Trust or its academies;
- Legislation, policy or strategies which will impact on privacy through the collection or use of information, or through surveillance or other monitoring;
- Purchasing/implementing cloud hosted applications;
- The collection of new data on an existing system;
- Setting up a CCTV system;
- The use of a new app that involves the sharing of pupil data;
- Processing of special category data
- Authorising the use of generative AI platforms.

A3.5 Steps to be followed when considering a new project

A DPIA should be undertaken before a project is underway, in the same way that we consider the cost impact of a project before making a commitment to spend any money. Colleagues should seek support from their data protection ambassador or the Head of Data Protection-and consider consulting with affected data subjects as a first step.

For academy projects, the DPIA process should be a collaborative task between the Headteacher, Data Protection Ambassador and colleagues who will be using the system/managing the project.

For Trust initiatives, the DPIA process will be a collaborative task between the colleague leading on the project with the support of the Head of Data Protection.

A3.6 Monitoring

The completed DPIA should be checked by the Head of Data Protection and then submitted to academy leadership (for academy projects) or Trust leadership (for Trust initiatives) for final review and approval.

In approving a DPIA, you are confirming that you are aware of the risks highlighted in the DPIA and are happy for the project to continue.

Where the residual risk remains high, despite the mitigating actions, it is a legal requirement to notify the ICO and to seek their approval before the project continues.

Once signed off the member of leadership will determine whether any risks highlighted in the DPIA should be added to the relevant academy or the Trust's risk register as appropriate. Regional Directors and the Audit and Risk Committee will also be consulted when necessary.

The DPIA, and the risks identified within the document, should be kept under review as deemed appropriate.