THIS POLICY COVERS ALL ACADEMIES/SCHOOLS WITHIN ARDEN MULTI-ACADEMY TRUST

Name of Policy	**DPIA Procedure**	
Lead	Martin Murphy, CEO	
Governor Committee	Business & Personnel Committee	
Policy Status	Taken from Browne Jacobson Policy	November 2025
	Trustee Approved	09/12/2025
Next Review	Autumn Term 2026	
Version No.	1	
Amendments		

Data Protection Impact Assessment Procedure

Introduction

This procedure sets out our procedures for Data Protection Impact Assessments (**DPIAs**). DPIAs are identified in our Data Protection Policy as a part of our data protection by design and default approach. All definitions contained within the Arden Multi-Academy Trust (Arden MAT) Data Protection Policy are applicable for this procedure.

DPIAs is a process to help the Arden MAT to identify data protection risks in relation to any new or changed ways of working that involve the processing of personal data. A DPIA, when carried out as part of integral project management plans, will help to identify and fix any data protection or security related issues early on in a project lifecycle. This reduces risks to data subjects, as well as reducing the risk of projects having unforeseen issues. Fixing issues when they have already occurred, as well as being detrimental to data subjects, can be more time consuming and costly to resolve, and incur risk to the organisation through damage to reputation, claims for damages from affected data subjects and regulatory action from the Information Commissioner's Office ("**ICO**").

In general, consistent use of DPIAs increases the awareness of privacy and data protection issues. It also ensures that all relevant staff involved in designing projects think about privacy at the early stages and adopt a data protection by design approach. A DPIA also brings broader compliance benefits, as it can be an effective way to assess and demonstrate compliance with all data protection principles and obligations. It can reassure individuals that the Arden MAT are protecting their interests and have reduced any negative impact on them as much as possible. In some cases, the consultation process for a DPIA gives data subjects a chance to have some say in the way their information is used. In turn, this can create potential benefits for the reputation of the Arden MAT and relationships with individuals.

There can also be financial benefits. Identifying a problem early on generally means a simpler and less costly solution, as well as avoiding potential damage later. A DPIA can also reduce the ongoing costs of a project by preventing duplication or minimising the amount of information collected and devising more straightforward processes for staff who will be carrying out the work identified in the DPIA.

The requirements for controllers to carry out DPIAs is set out in Articles 35 and 36 of the UK GDPR and the requirement for processors to assist the controller with the DPIA is set out in Article 28. The ICO provides detailed guidance on DPIAs on their website at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/ . This procedure has been created to comply with the requirements of the UK GDPR and takes into account the ICO guidance on DPIAs. It does not seek to duplicate the expert guidance of the DPO nor reproduce the legislation and guidance but to supplement it with information relevant to the Arden MAT to provide a useful procedure to follow.

This procedure sets out:

- What a DPIA means and what must be included in a DPIA;

- Information about when a DPIA must be conducted as required by the law and when we may carry out or review a DPIA as a matter of good practice;
- who is responsible for creating, reviewing and approving DPIAs.

What is a DPIA?

1 DPIAs are a process to systematically identify and minimise the data protection risks of a project, plan or way of working, throughout the lifecycle of a project where personal data is processed. Risk assessments are a familiar term to many school staff; DPIAs are a specialist risk assessment process. The DPIA process is a flexible process that provides the appropriate degree of assessment and mitigation in proportion to the nature and degree of risk involved.

2 DPIAs are not intended to be a one-off document-based exercise for approval or sign-off. Actions identified in the DPIA must be integrated back into project plans and followed throughout the whole project by those responsible for the data processing, including any decisions to stop processing personal data. DPIAs will need to be kept under regular review and updated if anything changes.

3 A DPIA can cover a single processing operation, or a group of similar processing operations, or an 'overarching' DPIA can be carried out for a group of similar processes e.g., one DPIA for the use of online learning platforms used by pupils.

4 A DPIA does not need to remove all risk from projects but are a useful tool to help determine whether or not the level of risk is acceptable in the circumstances when taking into account the benefits the processing is intended to achieve.

5 All new projects and ways of working, or changes to projects or ways of working must be screened to assess if a DPIA is required, using the questions set out in Annex 1 and records of the outcome must be passed to the DPO who is responsible for holding these records.

6 Whether a DPIA is either legally required, or carried out as a matter of good practice, a framework set of questions is set out in the Annex to this procedure to aid the completion of the DPIA. This contains suggestions for a framework for the DPIA process. However, completion of a prescribed template is not included as the process can be scaled up or down as required, proportionate to the nature of the risk. Simple DPIAs could be evidenced through minutes of a meeting, or more complex DPIAs could be incorporated into a broader project plan. All DPIA processes, regardless of format, must contain the following information:

6.1 The person/s or roles responsible for the project;

6.2 Whether the DPIA is being carried out due to a legal requirement i.e., where there is a high risk to data subjects, or whether the threshold has not been met, but a DPIA is being carried out as a matter of good practice;

6.3 A record of the DPO's advice in relation to the DPIA;

6.4 Description of the project including a description of the personal data to be processed;

6.5 A description of the significance of the processing, including whether particularly private personal data is to be processed, and/or personal data of vulnerable data subjects will be processed, and/or whether processing is likely to have a significant impact on data subjects;

6.6 Whether consultation with affected data subjects has been undertaken, and the results of that consultation, and if not carried out, why this is not considered appropriate;

6.7 Confirmation of the lawful basis for processing personal data;

6.8 How data subject rights will be upheld;

6.9 How the data protection principles will be implemented into the project;

6.10 A risk assessment describing any risks, the likelihood and severity of those risks being realised, an action plan setting how what needs to be done to mitigate the risk, who is responsible for completing the action and when it will be completed;

6.11 in relation to any outstanding overall project risk, whether that risk is a high risk. Where there are outstanding high risks for the project as a whole, it must be referred to the ICO for further consultation before processing commences;

6.12 How the DPIA will be kept under review over time, and any triggers for revisions of the DPIA.

7 Where relevant, the DPIA will also contain evidence of any due diligence processes where personal data will be shared with external parties, either as a processor or controller.

When to carry out a DPIA

8 DPIAs are legally required for new or changed processing of personal data that is likely to result in a high risk to the rights and freedoms of data subjects. In a school, high risks are likely to be identified in most projects due to the nature of the data subjects whose data is processed. The DPO will help data users identify where projects are likely to be high risk. Examples of high risk where a DPIA is legally required are:

8.1 Installation, or alteration to CCTV systems;

8.2 Biometric processing, such as fingerprint or facial recognition systems, which may be used for activities such as school meal payment, library systems or attendance registration;

8.3 Automated Intelligence systems where personal data is input into the system, either to train the model, or as part of use of the system;

8.4 Use of a new Edtech tool to monitor pupil and staff IT usage, for example, a system monitoring all keystrokes on school IT equipment or when connected to school systems for safeguarding purposes;

8.5 Use of Edtech systems, including learning and assessment platforms which are connected to the school management information system to allow pupil accounts or profiles to be automatically created when a pupil joins the school;

8.6 A new HR record-keeping system;

8.7 New or changed data storage systems (such as moving from an on-premise to cloud-based storage system, or changing cloud-based storage providers);

8.8 A new database which consolidates information previously held by separate parts of the Arden MAT;

8.9 Where data processed relates to vulnerable subjects including children. Employees can also be considered vulnerable individuals due to the employer/employee student/staff power imbalance meaning they cannot easily consent or object to the processing of their data.

9 Where the Arden MAT are not legally required to carry out a DPIA, data users may still choose to carry out one as a matter of good practice and/or on the advice of the DPO.

10 DPIAs will be carried out as early as possible when planning or changing projects or ways of working and data users will not commence a project without ensuring the DPIA process is completed.

11 Data users may identify an existing project or way of working that has not previously been reviewed using the DPIA process, but an assessment of the processing indicates that a DPIA would be legally required or a matter of good practice. In these cases, the data user should consult with the DPO, who may advise that the processing activity should continue but may advise that a DPIA process to review the risks and mitigations in relation to that processing is carried out at the earliest opportunity.

12 As part of the DPIA process, the review triggers for that process will be identified, which may be time-based, or event-based. Additionally, a review may also be undertaken if new risks become apparent, for example, if there is a personal data breach, identification of security flaws or stakeholders raise concerns over the processing.

Who is responsible for a DPIA?

13 Data users managing projects to implement new (or update existing) systems or procedures which involve the processing of personal data, are responsible for:

13.1 Identifying if a DPIA is required by completing the screening process set out in Annex 1;

13.2 Seeking advice on the DPIA from the DPO and completing the DPIA with the assistance of the DPO and other appropriate people or teams (e.g., the IT team, MIS staff, classroom practitioners);

13.3 Ensuring completion and monitoring of the tasks allocated to them in the action plan;

13.4 Ensuring on-going compliance with the outcomes of the DPIA and bringing any changes to processing, additional risks or concerns to the attention of the DPO.

14 The DPO is responsible for:

14.1 Supporting data users to complete the DPIA, providing advice on the identification and mitigation of risks and assigning a suitable person/role to be responsible for any actions identified;

14.2 Providing advice in relation to the DPIA and ensuring that the advice is recorded;

14.3 Keeping a record of risks and where appropriate, entering them onto the Arden MAT risk register;

14.4 Monitoring the performance of the DPIA process, including screening outcomes, and the outcomes of DPIAs;

14.5 Where a project is identified as being high-risk even after mitigating action is completed, advising that the ICO is consulted in relation to that processing and then acting as point of contact for the ICO in relation to that consultation;

14.6 Providing expert advice regarding internal management sign-off for the project, which the DPO may consider, depending on the nature of the project and the risk, can be signed off at a departmental, school leader or governance level.

14.7 Ensuring that evidence of the DPIA process is retained, that any new activities are added to the Record of Processing Activities, retention policies, retention procedures and relevant privacy notices are updated.

15 The Arden MAT board are responsible for strategic oversight of data protection compliance, which may include asking questions about the DPIA process, which projects and ways of working have been subject to a DPIA, asking if DPIAs have been considered as part of any procurement processes which they may be involved in approving, and for higher-risk projects, reviewing the DPIA and providing management sign-off for any outstanding risks.

Annex 1 DPIA Screening Checklist

NAME OF PROJECT:

NAME OF MEMBER OF STAFF COMPLETING THIS SCREENING:

DATE:

Question	Example	YES/NO
Is this a major project involving the use of personal data?		
Do you plan to carry out any:		
evaluation or scoring	Automated scoring of job applications	
automated decision-making with significant effects (for example,	Automated processing of pupil applications for 6th form places	
systematic monitoring	CCTV systems (new or extension of existing systems)	
processing of sensitive data or data of a highly personal nature	information about children's health data or safeguarding information	
processing on a large scale	More than 1000 data subjects	
processing of data concerning vulnerable data subjects	Children are vulnerable data subjects and employees may also be due to the imbalance of power between employee and employer	
innovative technological or organisational solutions	AI to make recruitment decisions	
use systematic and extensive profiling or automated decision-making to make significant decisions about people	Using automated tools to assess if pupil has ADHD	
process special-category data or criminal-offence data on a large scale	Processing information about pupils who have SEND on a trust-wide basis	

Question	Example	YES/NO
use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit	AI to make recruitment decisions	
carry out profiling on a large scale	Using an online system to predict and set pupil target GCSE grades	
process biometric or genetic data	Fingerprint or facial recognition technology	
process personal data in a way that involves tracking individuals' online or offline location or behaviour	Routine monitoring of keystrokes on school IT equipment for safeguarding monitoring	
process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them	Sharing children's personal data with external tutoring providers so	
process personal data that could result in a risk of physical harm in the event of a security breach	This could include relatively low risk activities such as pupil edtech accounts if pupils are in hiding and their personal safety were to be at risk if it were to be revealed where they attend school	
Is there is a change to the nature, scope, context or purposes of existing processing where it meets the criteria above?		

If the answer to **any** of these questions is YES, then this indicates that a DPIA is a legal requirement. Please seek the advice of the DPO and see Annex 2, the outline of a DPIA for support to get you started on the DPIA process.

If the answer to these questions are **all** NO, but you are still not sure, or think a DPIA may be required as a matter of good practice and to support you with your project please seek the advice of the DPO. Remember, even if a DPIA is not legally required, you should still consider any risk and ensure that the data protection principles are followed. A DPIA

Please keep a record of this process for your own records and send it to the DPO who can retain it as evidence of the DPIA process.

Annex 2 DPIA framework

Front page

- Organisation name
- Author(s)
- Version history
- DPO Advice (put this on the front page so it can easily be found)
- Is a DPIA legally required or is it being carried out as good practice
- Sign off from suitable senior lead (this may vary depending on the nature of the project and the risks)

Introduction

Description of the project

- What is being proposed
- How will data now be processed differently
- What is the current way of working
- Is this new/changed processing necessary OR what will be improved by this new way of working that makes this changed/increased risk worthwhile

How is data processed

- Personal data processed
  - Whose PD
  - What PD
  - How will this be processed/shared
  - Who is data controller
  - Are data processors involved? Sub-processors?
  - Where will data be stored- any international transfers
  - What due diligence has been done on any external parties (refer to annex)
- Lawful basis
  - Article 6

- Article 9 (plus DPA 2018 condition if required)

- Data subject rights
  - Which rights are relevant
  - How will data subjects be able to exercise their rights
- Significance of processing
  - Is this processing likely to raise privacy concerns
  - Are data subjects considered to be vulnerable
  - Is the processing likely to have a significant impact on data subjects
  - What consultation has been done with stakeholders (if not, why not)

Risk Assessment

(For higher risk projects, it is advisable to risk assess against each of the principles in turn, so nothing is accidentally omitted)

The principles are:

- Lawful, fairness and transparency
  - Lawful basis- this should be clear from part 1 narrative
  - Fairness- is this fair to data subjects- this should be clear from part 1 narrative
  - Transparency- how are you informing data subject about this processing- do privacy notices need to be updated or any extra transparency work
- Purpose limitation
  - For what purpose was the data originally collected- if not for this purpose, is this new purpose compatible
  - How to ensure data is not then used for a further incompatible purpose
- Data adequacy/minimisation
  - Is adequate data being collected for this purpose
  - Can each data element being processed be justified- any excessive collection
- Accuracy
  - Is data accurate
  - How will data be kept accurate over time
- Storage limitation

    - How long will data be retained for
    - If external parties are included, how long will they retain data for
    - What arrangements are in place to ensure data deleted/destroyed when no longer needed
- Security
    - What arrangements are in place to ensure data is kept securely. Remember to include explanation of technical (e.g. encryption) and organisational (e.g. training) measures
    - If external parties are involved, refer to their measures as evidenced by due diligence

For each of the risks:

- describe the risk,
- what mitigations are already in place
- state remaining impact and likelihood of risk occurring (risk matrix may be used if appropriate, see below)
- what additionally needs to be done to mitigate the risk (the action required).

Action Plan

For each action:

- Who is responsible for the action
- What monitoring and ongoing work will be done to ensure the mitigations are ongoing and to keep this DPIA under review
- State residual risk (impact and likelihood) for each outstanding risk
- State residual risk for project as a whole (if high risk, must consult ICO)

Due Diligence Annex (If relevant)

- Evidence of due diligence for each external party
    - Vendor contracts (data processing or sharing agreements)
    - Vendor documentation- privacy notices, privacy policies, additional information
    - Vendor security information (completed vendor security questionnaire)
- What arrangements are in place to continue to review vendor compliance.

Risk Matrix (*which may be used if helpful*)

LIKELIHOOD	IMPACT					
		Trivial	Minor	Moderate	Major	Severe
	Almost Certain	Low Med	Medium	High	Very High	Very High
	Likely	Low	Low Med	Med High	High	Very High
	Possible	Low	Low Med	Medium	Med High	High
	Unlikely	Low	Low Med	Low Med	Medium	Med High
	Rare	Low	Low	Low Med	Medium	Medium
Impact x Likelihood = Risk						