The Wilnecote School

Title: DPIA Policy

Member of leadership team with lead responsibility for oversight and update of policy	Mr. M Stevenson
Approved at SLT	July 2026
Policy approval at Governing Body	July 2026
Policy review cycle	Bi-annually
Policy review date	July 2028

Purpose

The purpose of this policy is to ensure that privacy risks to individuals are identified, assessed, and appropriately mitigated whenever new or changed processing of personal data is proposed, in accordance with:

- The UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act 2018
- The Data (Use and Access) Act 2025 (DUAA)

A Data Protection Impact Assessment (DPIA) enables the organisation to:

- Comply with statutory data protection obligations
- Identify and reduce risks to individuals' rights and freedoms
- Embed privacy, fairness, and accountability into decision-making
- Support responsible data use, innovation, and data sharing where appropriate
- Demonstrate compliance to regulators, partners, and stakeholders

Scope

This policy applies to:

- All new projects, systems, services, or initiatives involving personal data
- Any significant change to existing processing activities
- All staff, contractors, and third parties acting on behalf of the organisation

It covers all forms of personal data, including:

- Digital and paper records
- Student, staff, contractor, and third-party data
- Special category and criminal offence data
- Processing involving automated decision-making or profiling

The policy applies regardless of whether processing relies on consent, contractual necessity, public task, legitimate interests, or recognised legitimate interests introduced by the DUAA.

When a DPIA Is Required

A DPIA must be completed before processing begins where a project or change is likely to result in high risk to individuals, including (but not limited to):

- Introduction of new or significantly changed systems or technologies
- Large-scale processing of personal data
- Processing of special category or criminal offence data
- Systematic monitoring, profiling, or automated decision-making with legal or similarly significant effects
- Data sharing with new third parties or external partners
- Re-use of personal data for purposes beyond the original intent
- Use of personal data in ways individuals would not reasonably expect

The DUAA confirms that existing DPIA thresholds remain unchanged, including for research, statistical analysis, and innovation-related processing.
Where there is uncertainty, advice must be sought from the Data Manager or Data Protection Officer (DPO).

Roles and Responsibilities

Senior Leadership Team (SLT)

- Provide strategic oversight of data protection and data use risk
- Ensure appropriate resources and controls are in place
- Approve projects with residual medium or high privacy risk
- Ensure organisational readiness to meet regulatory expectations under DUAA

Academic Board

- Provide oversight where DPIAs relate to academic activity, teaching, research, or assessment
- Ensure data protection and ethical data use are embedded within academic governance

Project Owner / Lead

- Identify when a DPIA is required
- Complete the DPIA accurately and at the earliest stage of project planning
- Ensure lawful basis (including recognised legitimate interests, where relevant) is clearly documented
- Implement risk mitigation actions prior to project approval and go-live

Data Manager / Data Protection Officer

- Advise on DPIA requirements and lawful bases for processing
- Review DPIAs for compliance, proportionality, and adequacy of safeguards
- Escalate high-risk or non-mitigated processing to SLT
- Monitor developments in ICO guidance relating to DUAA implementation

All Staff

- Comply with this policy and associated procedures
- Escalate any data protection concerns promptly

DPIA Process

A DPIA must follow a documented and proportionate process:

1. Identify the need for a DPIA at the earliest planning stage
2. Describe the processing, including:
    - Purpose and expected benefits
    - Data types, data subjects, and volumes
    - Legal basis (including recognised legitimate interests, where applicable)
3. Assess necessity and proportionality, including purpose compatibility under DUAA
4. Identify risks to individuals' rights and freedoms
5. Define mitigation measures, safeguards, and controls
6. Assess residual risk and determine escalation requirements
7. Obtain approval before processing begins
8. Review and update the DPIA if processing changes

No project may proceed where unacceptable risk remains untreated.
The DUAA confirms that DPIA requirements remain a core accountability measure under UK GDPR and DPA 2018.

Consultation and Escalation

Where a DPIA identifies:

- High risk
- Novel, large-scale, or sensitive processing
- Significant automated decision-making
- Processing involving children or vulnerable individuals

Monitoring and Review

This policy will be:

- Reviewed periodically
- Updated to reflect legislative changes, including DUAA commencement phases
- Revised following publication of new ICO guidance or codes of practice

Compliance with this policy forms part of the organisation's wider information governance and accountability framework.