PARSLOES PRIMARY SCHOOL

DATA PROTECTION IMPACT ASSESSMENT POLICY

Document Type	Approved
Author	Data Protection Officer
Owner	Headteacher
Document Version	Version 5
Created	August 2025
Approved by	Governing Body
Review Date	August 2028 or earlier where there is a change in the applicable law affecting this Policy Guidance

Version Control:

Version	Date	Author	Description of Change
1	30/08/2018	Data Protection Enterprise www.dataprotectionenterprise.co.uk	New Policy
2	01/08/2019	Data Protection Enterprise Ltd www.dataprotectionenterprise.co.uk	Annual Review Amendments to: organisation amended to read School
3	21/09/2020	Data Protection Enterprise Ltd www.dataprotectionenterprise.co.uk	Annual Review S 11 Links to other policies added
4	20/01/2022	Data Protection Enterprise Ltd www.dataprotectionenterprise.co.uk	GDPR 2016/679 to UK GDPR
5	August 2025	Data Protection Enterprise Ltd www.dataprotectionenterprise.co.uk	Annual Review: Amendments to: S3 – last paragraph deleted S4.2 and 4.3 amended Section 9 added

Contents:

1. INTRODUCTION & PURPOSE

DOCUMENT STATEMENT AND AIM

This policy sets out the principles by which we will develop, manage, and review the management of Data Protection Impact Assessments (DPIA).

A DPIA is a process designed to help the school systematically analyse, identify and minimise the data protection risks of a project or plan. It enables the School to identify and resolve problems at an early stage, reducing associated costs and reputational damage that might otherwise occur.

It is as important that a DPIA is carried out when planning changes to processes that handle personal confidential data, as well as when planning the implementation of new systems.

The purpose of this policy is to:

- Establish a consistent, documented approach to conducting DPIAs
- Ensure compliance with UK data protection legislation
- Demonstrate the School's commitment to privacy by design and default principles
- Provide clear guidance to staff on when a DPIA is required and what to do
- Minimise risks to individuals' privacy, confidentiality and data security
- Document decisions made about data protection risks.

2. SCOPE

This policy applies to all staff, governors, volunteers and contractors who process personal data on behalf of the school. It covers all processing of personal data, whether in electronic form or in paper records, where a new process, system or project is being implemented or where significant changes are being made to existing processes.

Any new use of AI tools or systems that process personal data will be assessed through the DPIA process to evaluate and manage any data protection risks. This includes generative AI tools, learning analytics platforms, or predictive systems used in the School's operations.

3. EQUALITY AND HUMAN RIGHTS STATEMENT

The School is committed to ensuring that all data processing activities are conducted with appropriate consideration for equality and human rights.

When conducting Data Protection Impact Assessments, the school will:

- Consider the potential for differential privacy impacts on individuals with protected characteristics under the Equality Act 2010
- Assess whether proposed processing might inadvertently discriminate against or create barriers for particular groups
- Ensure that privacy solutions do not themselves create or exacerbate inequality
- Consider accessibility requirements when implementing privacy controls or communications

- Pay particular attention to the rights and needs of vulnerable individuals, including children and those with special educational needs and disabilities
- Balance data protection requirements with other rights, including the right to education

The School recognises that effective data protection supports fundamental rights to privacy and data protection while enabling the educational mission of the school to be fulfilled in an equitable manner.

This approach ensures compliance with both data protection legislation and the Public Sector Equality Duty under the Equality Act 2010.

4. LEGAL FRAMEWORK

This policy is based on the following legislation and guidance:

- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Data Use and Access Act 2025 (DUAA)
- Information Commissioner guidance on DPIAs
- Relevant Department for Education (DfE) guidance

5. WHEN IS A DPIA REQUIRED

A DPIA must be carried out:

1. **When required by law**: UK GDPR requires a DPIA if the processing is "likely to result in a high risk to the rights and freedoms of natural persons."

2. **Specifically, a DPIA is required when the school plans to**:

    - Use systematic and extensive profiling or automated decision-making to make significant decisions about people
    - Process special category data or criminal offence data on a large scale
    - Systematically monitor publicly accessible places on a large scale
    - Use new technologies or innovative applications
    - Use profiling or special category data to decide on access to services
    - Process biometric or genetic data
    - Match data or combine datasets from different sources
    - Process personal data without providing a privacy notice directly to the individual
    - Process children's personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them
    - Process personal data that could result in a risk of physical harm in the event of a security breach

3. **School-specific processing activities that may require a DPIA**:

- Implementation of new student information systems

- Introduction of biometric systems (e.g., fingerprint scanners for library access, catering)
- Implementation of CCTV systems
- Creation of systems for monitoring staff or student activity
- New data sharing initiatives between schools or with external organisations
- Introduction of new technologies, such as AI-driven learning tools
- Changes to existing systems that significantly alter how personal data is processed

6. DPIA PROCESS

6.1 Identification of Need

The need for a DPIA should be identified early in the planning process for any new initiative, system, or significant change to existing processes that involve personal data.

The School Data Protection Officer (DPO) should be consulted at the outset to help determine whether a DPIA is required.

6.2 DPIA Team

The DPIA will be carried out by the DPO with the appropriate expertise and knowledge of the project that may include:

- The project lead/manager
- IT manager
- Senior leadership representative
- School Business Manager

6.3 DPIA Steps

The School will follow these key steps when conducting a DPIA:

Step 1: Describe the Processing

Provide the DPO with the following information:

- Describe the nature, scope, context and purposes of the processing
- Identify what personal data will be collected and used
- Identify the data subjects (e.g. pupils, staff, parents)
- Describe how the data will be collected, used, stored and deleted
- Identify which systems will be used to process the data

Step 2: Assess Necessity and Proportionality

The DPO will:

- Determine whether the processing is necessary and proportionate for the purpose
- Identify the lawful basis for processing

- Ensure compliance with the UK GDPR, DPA and DUAA
- Consider how to ensure data quality and data minimisation are in place
- Explain how individuals will be informed about the processing where necessary
- Document how data subject rights will be upheld
- Ensure compliance with data protection principles
- Ensure data processors comply with data protection legislation and requirements

Step 3: Identify and Assess Risks

The DPO will:

- Identify potential risks to individuals' rights and freedoms
- Assess the likelihood and severity of each risk
- Consider risks from both internal and external perspectives
- Document the potential impact of each risk
- Document retention periods
- Identify any data sharing that will take place

Step 4: Identify Measures to Mitigate Risks

The DPO will:

- Identify controls to address each risk
- Evaluate the resulting level of risk after mitigation
- Implement additional safeguards where necessary
- Document all decisions made

Step 5: Recommendation and Implementation

The DPO will:

- Make a recommendation regarding whether to proceed with the processing
- Identify any changes needed before proceeding
- Document all decisions

Step 6: Sign off

On completion of the DPIA the DPO will:

- Submit the completed DPIA for review and approval
- Obtain sign-off from the appropriate authorised person(s)
- For high-risk processing that cannot be mitigated, consult with the ICO

Step 7: Integration into Project Plan

The School should:

- Ensure that the recommended actions are integrated into the project plan where appropriate
- Assign responsibilities for implementing mitigations
- Set timelines for implementation

Step 8: Review

The DPO will be responsible for the review of the DPIA and make adjustments as necessary.

7. ROLES AND RESPONSIBILITIES

7.1 Data Protection Officer (DPO)

- Provide advice and guidance on when a DPIA is required
- Completion of DPIAs
- Review completed DPIAs and provide recommendations
- Maintain a register of all DPIAs conducted
- Determine whether consultation with the ICO is required

7.2 Senior Leadership Team

- Ensure DPIAs are conducted when required
- Review and approve high-risk DPIAs
- Ensure recommended actions are implemented
- Foster a culture of privacy by design

7.3 Project Managers

- Contact the DPO at the outset
- Provide the necessary information of the project to support the DPO

7.4 All Staff

- Be aware of when a DPIA might be required
- Alert the DPO to new projects or changes that might require a DPIA
- Contribute to the DPIA process when requested
- Comply with measures identified in the DPIA

8. DPIA TEMPLATE AND REGISTER

The DPO will use a standardised template for conducting DPIAs.

The DPO will maintain a central register of all DPIAs conducted. This register will record:

- Project name and description
- Date DPIA completed
- Summary of risks identified and measures implemented
- Review date
- Approval details

9. CONSULTATION

Where appropriate, the school will seek the views of data subjects or their representatives on the intended processing. This might include:

- Pupil consultations (where age-appropriate)
- Parent consultations
- Staff consultations
- Governors' consultations

10. OUTCOMES

A DPIA may result in one of the following outcomes:

- Proceed with the proposed processing – where risks are adequately mitigated
- Modify the proposal – to reduce risks to an acceptable level
- Abandon the proposal – where risks cannot be sufficiently mitigated and the processing cannot be justified

11. PRIOR CONSULTATION WITH THE ICO

Where a DPIA identifies high risks that cannot be sufficiently mitigated, the DPO will consult with the ICO before proceeding with the processing. The DPO will:

- Prepare documentation for the ICO
- Submit the consultation request
- Liaise with the ICO during the consultation period
- Communicate the outcome to relevant stakeholders

12. RECORD KEEPING

All DPIAs will be:

- Documented in writing
- Stored securely with appropriate access controls
- Retained in line with the school's retention schedule
- Made available to the ICO upon request

13. POLICY REVIEW

The DPO is responsible for monitoring and reviewing this policy. Although this policy is reviewed every three years, changes to legislation, national guidance, codes of practice or advice from the Information Commissioner advice may trigger interim reviews. The DPO will

highlight any significant legislative developments that may require earlier action or updates to this Policy.

14. LINKS WITH OTHER POLICIES

This Data Protection Impact Assessment policy is linked to the Schools:

- Data Protection Policy
- Freedom of information Policy
- Security Incident and Data Breach Policy
- CCTV Policy
- Information Sharing Policy
- Information Security Policy
- Safeguarding policy
- UK GDPR Privacy Notices

The Information Commissioner also provides a free helpdesk that can be used by anyone and a website containing a large range of resources and guidance on all aspects of Information Law for use by organisations and the public. See Information Commissioner.