John Perry Primary School

DATA PROTECTION IMPACT ASSESSMENT POLICY

If printed, copied or otherwise transferred from the Policies and Procedures Intranet/Internet Site this document must be considered to be an uncontrolled copy.

Policy amendments may occur at any time and you should consult the Policies and Procedures Intranet/Internet Site if in doubt.

Approved by: School Governing Body **Date:**

Last reviewed on: August 2024

Next review date: September 2027

Controlled Document

Title	Data Protection Impact Assessment Policy
Author	Data Protection Officer
Owner	Headteacher
Subject	Data Protection Impact Assessment Procedure
Document Version	Version 3
Created	August 2024
Review Date	September 2027 or earlier where there is a change in the applicable law affecting this Policy Guidance

Version Control:

Version	Date	Author	Description of Change
1	29/08/2020	Data Protection Enterprise Ltd www.dataprotectionenterprise.co.uk	New Policy
2	29/08/2021	Data Protection Enterprise Ltd www.dataprotectionenterprise.co.uk	General Data Protection Reglation 2016/679 is amended to read UK General Data Protection Regulation
3	01/08/2024	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
2. Scope
3. Equality and Human Rights Statement
4. Roles and Responsibilities
5. Governance Arrangements
6. Principles of Application
7. Policy Audit and Monitoring Compliance
8. Statement of Evidence/References
9. Policy Review
10. Links to other policies

1. INTRODUCTION

DOCUMENT STATEMENT AND AIM

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

The Information Commissioner defines a Data Protection Impact Assessment (DPIA) as:

'a process which helps assess privacy risks to individuals in the collection, use and disclosure of information. DPIA's help identify privacy risks, foresee problems and bring forward solutions.'

A DPIA is a tool that allows for proper planning for the effective implementation of new or changed systems in a way that assures the confidentiality, security, and integrity of Personal Confidential Data and/or Business sensitive data.

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.

2. SCOPE

This procedure applies to all staff and all processes that include a new or changed use of Personal Confidential Data and/or Business sensitive data in any format.

Typical examples are:

- introduction of a new paper or electronic information system to collect and hold personal/business sensitive data;
- introduction of new service or a change to existing process, which may impact on an existing information system.
- update or revision of a key system that might alter the way in which the School uses, monitors, and reports personal/business sensitive information.
- replacement of an existing data system with new software
- changes to an existing system where additional personal/business sensitive data will be collected
- proposal to collect personal data from a new source or for a new activity
- plans to outsource business processes involving storing and processing personal/ business sensitive data
- plans to transfer services from one provider to another that include the transfer of information assets
- any change to or introduction of new data sharing agreements

3. EQUALITY AND HUMAN RIGHTS STATEMENT

Promoting equality, eliminating unfairness and unlawful discrimination, and treating colleagues, partners and the public with dignity and respect, are fundamental to successful performance by all staff in the Trust, who are all expected to actively promote equality and

human rights and challenge racism, homophobia, and other forms of discrimination through their activities, and support others to do the same.

All staff are expected to work with others on effective approaches to ensure strategies, policies and activities promote and demonstrate equality and human rights.

Equality Impact Assessment and Equality Analysis are to be used as part of developing and monitoring proposals and projects for their impact on equality and equity.

4. ROLES AND RESPONSIBILITIES

4.1 HEADTEACHER

The Headteacher is responsible for ensuring that DPIA's are carried out for all new or changed uses of Personal Confidential Data as stated above and must sign off each DPIA.

4.2 BUSINESS MANAGERS AND INFORMATION ASSET OWNERS

The School Business Manager (or school equivalent) and Information Asset Owners are responsible for ensuring that new projects or changed ways of working include a DPIA in line with the policy and law noted below.

4.3 STAFF

All staff working in a new or changed way of working with personal confidential data shall engage with the school Data Protection Officer to ensure that a DPIA is completed satisfactorily and in compliance with data protection law.

5. GOVERNANCE ARRANGEMENTS

OVERSIGHT

The Oversight of this procedure is with the Data Protection Officer where Information Governance is reviewed, along with the DPIA log and any associated documentation including questionnaires and reports. The Data Protection Officer will complete the questionnaires and DPIA's as necessary to the new or changed use of personal confidential data and provide recommendations as necessary prior to approval by the Headteacher.

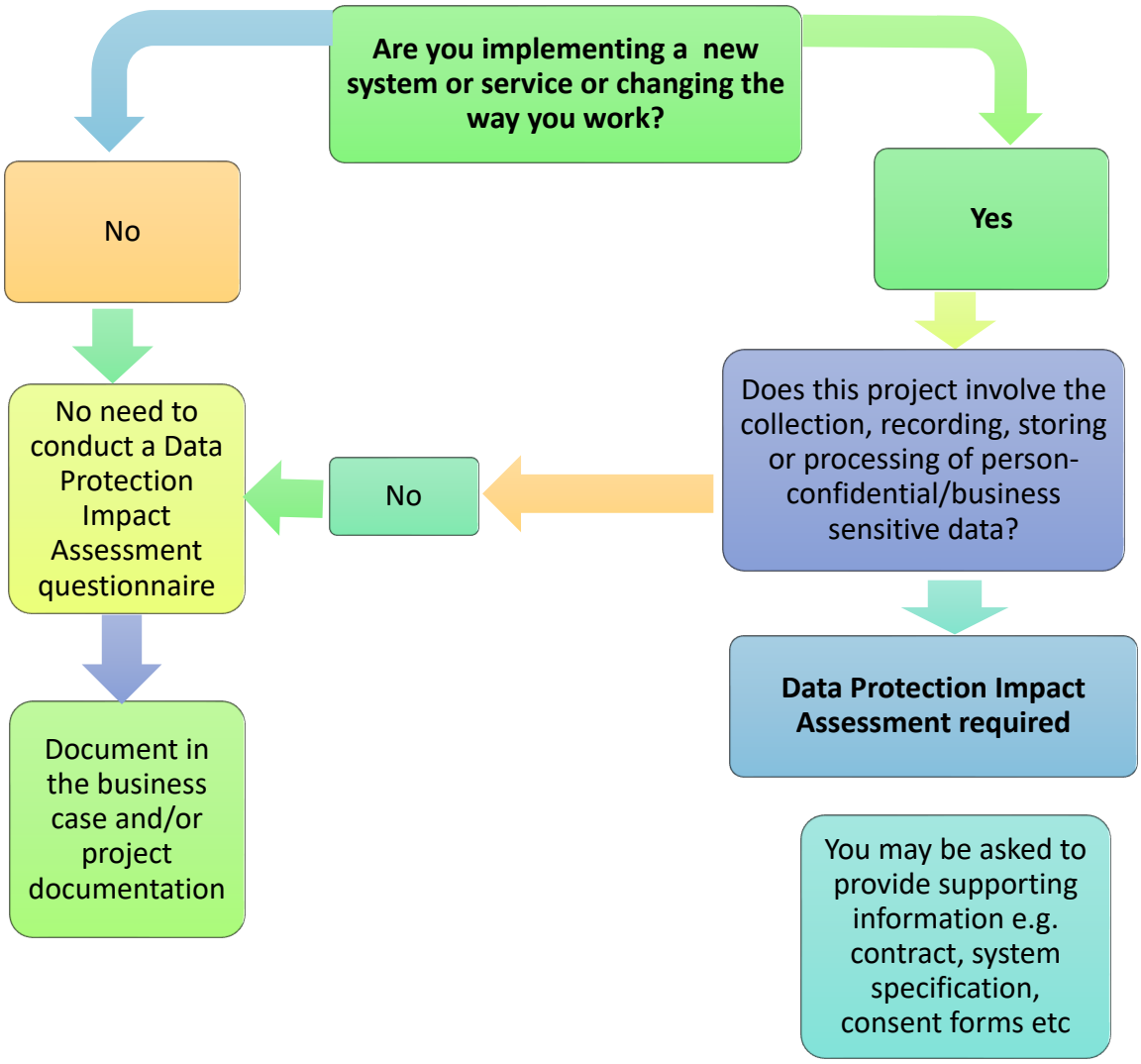
6. PRINCIPLES OF APPLICATION

6.1 IMPLEMENTATION

Prior to the start of a new or changed use of Personal Confidential Information, the data protection officer will complete a DPIA questionnaire, which allows for the risk assessment of the project to take place before costs are incurred and for any information risk to be monitored throughout the project.

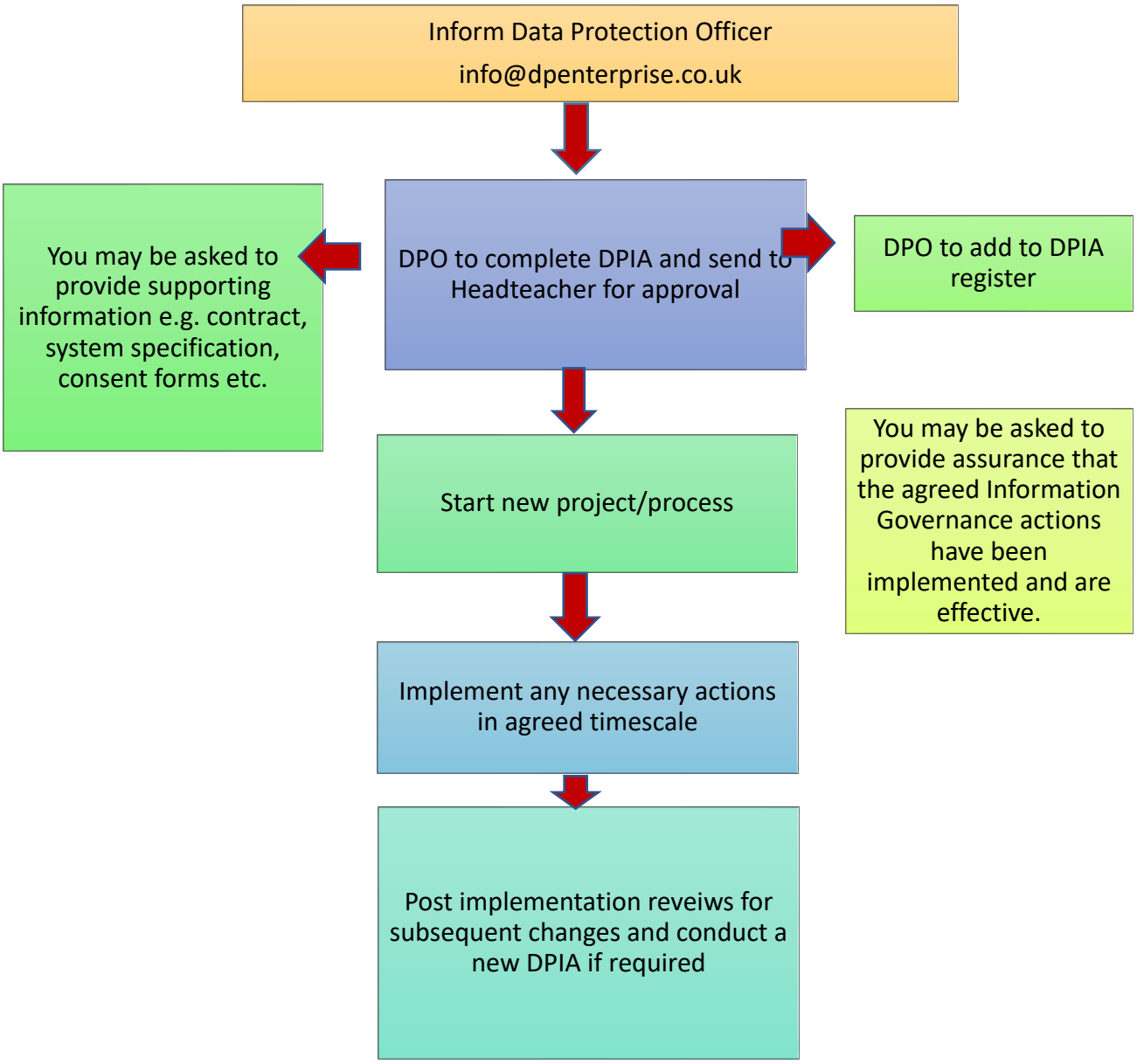
The following flow chart shows the questions to be answered to determine whether a DPIA questionnaire is required. Where a DPIA questionnaire is identified as NOT being required, this must be documented in the business case and/or project documentation of the new or changed system/process.

Does this project involve the collection, recording, storing or processing of person-confidential/ business sensitive data?



6.2 THE DPIA PROCESS

The DPIA process can be displayed as the process diagram below. All stages of the process must be followed in order to ensure proper use of Personal Confidential Data/Business Sensitive Data.



6.3 STAKEHOLDER ENGAGEMENT

Engagement with key stakeholders throughout the DPIA process ensures all parties are aware of, and will approve, access to personal confidential data without delaying the project. Good communication leads to better understanding of any information sharing and security issues. The DPIA process has the added advantage of propagating a common understanding of the

principles and basis for using and sharing personal confidential data/business sensitive data lawfully and ethically, helping the project to run more smoothly.

If a high risk is identified that cannot be mitigated, then the Data Protection Officer will consult with the Information Commissioner before starting the processing. The Information Commissioner will give written advice within eight weeks, or 14 weeks in complex cases.

6.4 DETERMINE

Members of staff should establish and document:

- The purpose of processing the data
- Who are the Data Controllers (sole, joint or in common) and Data Processors (see below for details)
- The legal basis for sharing the information, i.e. consent or another legal basis

The information types (data fields and classes), how the data will flow and where it will be held, what the risks are to its security when in transit and at rest, and what will happen to it once the purpose has been achieved (the information lifecycle).

6.5 DESIGN

Once the determination stage is complete and all the relevant information is collated, the design stage incorporates the following:

- Security standards governing the shared information, and who will be responsible
- System operation
- Stakeholder/End User materials

Care should be taken to ensure that information is handled in accordance with the School policy and within the bounds of the relevant laws. The UK GDPR has 6 Principles to be adhered to.

6.6 DEPLOYMENT

Physical sharing or 'go live' of the data sharing or new procedure can only take place once the first two sections are complete and signed off by the relevant stakeholders. A DPIA report should be created to collate the steps taken in creating the safe environment for the information to be shared.

7. POLICY AUDIT AND MONITORING COMPLIANCE

The Data Protection Officer is responsible for reviewing this Data Protection Impact Assessment Policy.

8. STATEMENT OF EVIDENCE/REFERENCES

The legislation and national guidance relevant to this procedure:

- Data Protection Act 2018
- The UK General Data Protection Regulation
- Information Commissioner Guidance for Data Protection Impact Assessments
- Information Sharing Policy

9. POLICY REVIEW

The Data Protection Officer is responsible for monitoring and reviewing this policy. In addition, changes to legislation, national guidance, codes of practice or commissioner advice may trigger interim reviews.

10. LINKS WITH OTHER POLICIES

This Data Protection Impact Assessment policy is linked to our:

- 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