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 2021

Next review date: September 2024

Controlled Document

Title	Data Protection Impact Assessment Policy
Author	Data Protection Officer
Owner	Headteacher
Subject	Data Protection Impact Assessment Procedure
Government Security Classification	Official
Document Version	Version 2
Created	August 2021
Review Date	September 2024 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

Contents:

1. INTRODUCTION

DOCUMENT STATEMENT AND AIM

This procedure sets out the principles by which John Perry Primary School (hereinafter referred to as the School) will develop, manage, and review the management of Data Protection Impact Assessments (DPIA)

The Information Commissioner's Office 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 School, 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.

All staff, including the Governors are required to abide by all equality and human rights legislation and good practice, and will receive appropriate training and support to do so.

4. ROLES AND RESPONSIBILITIES

4.1 HEAD TEACHER AND SCHOOL GOVERNORS

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 Business Manager 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 ensure that a DPIA is completed following the appropriate process outlined in the flow chart below.

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 receive the questionnaires and DPIAs as necessary to the new or changed use of Personal Confidential Data and provide recommendations as necessary prior to approval by the Headteacher.

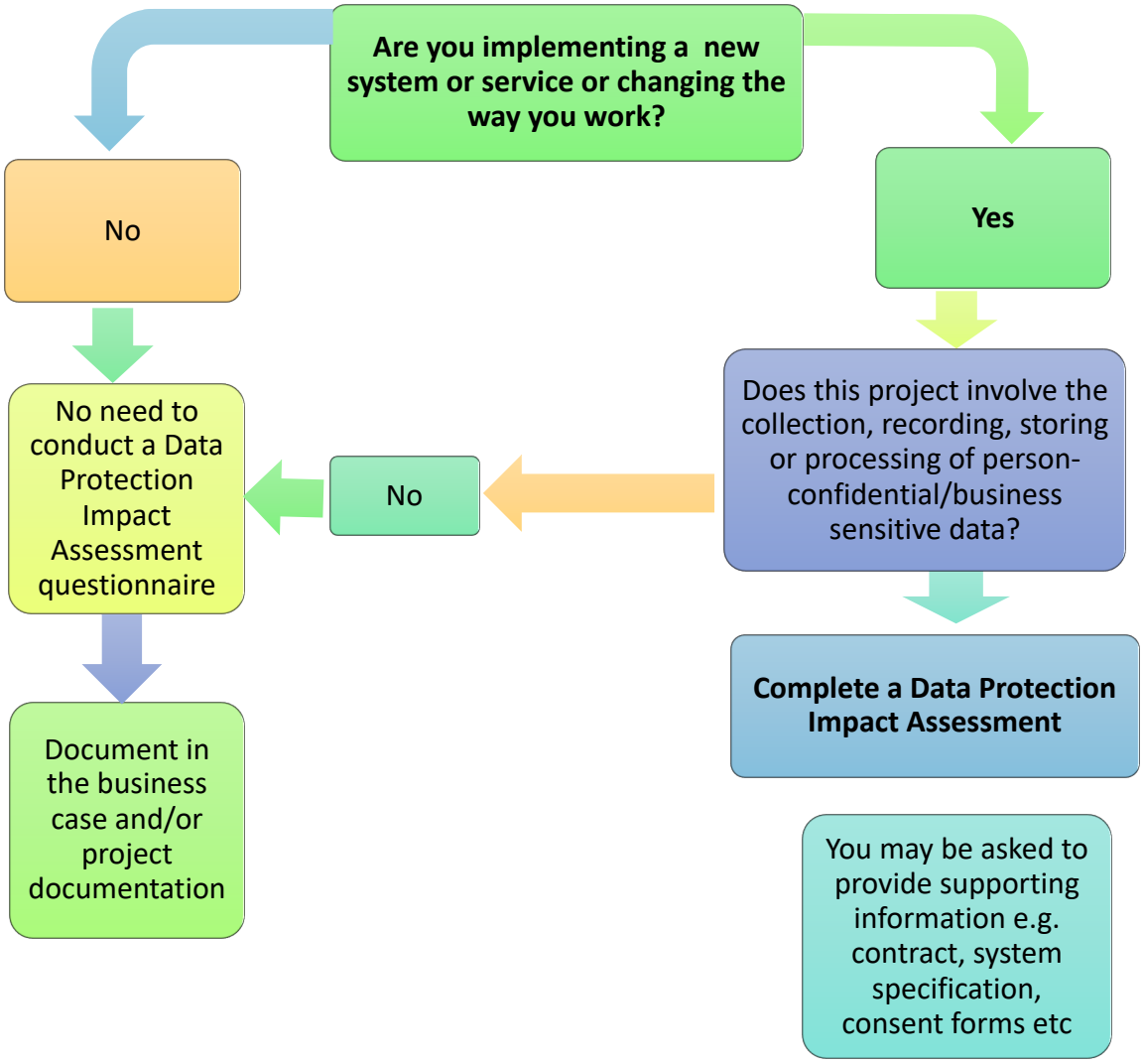
6. PRINCIPLES OF APPLICATION

6.1 IMPLEMENTATION

Prior to the start of a new or changed use of Personal Confidential Information, the responsible person must 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?

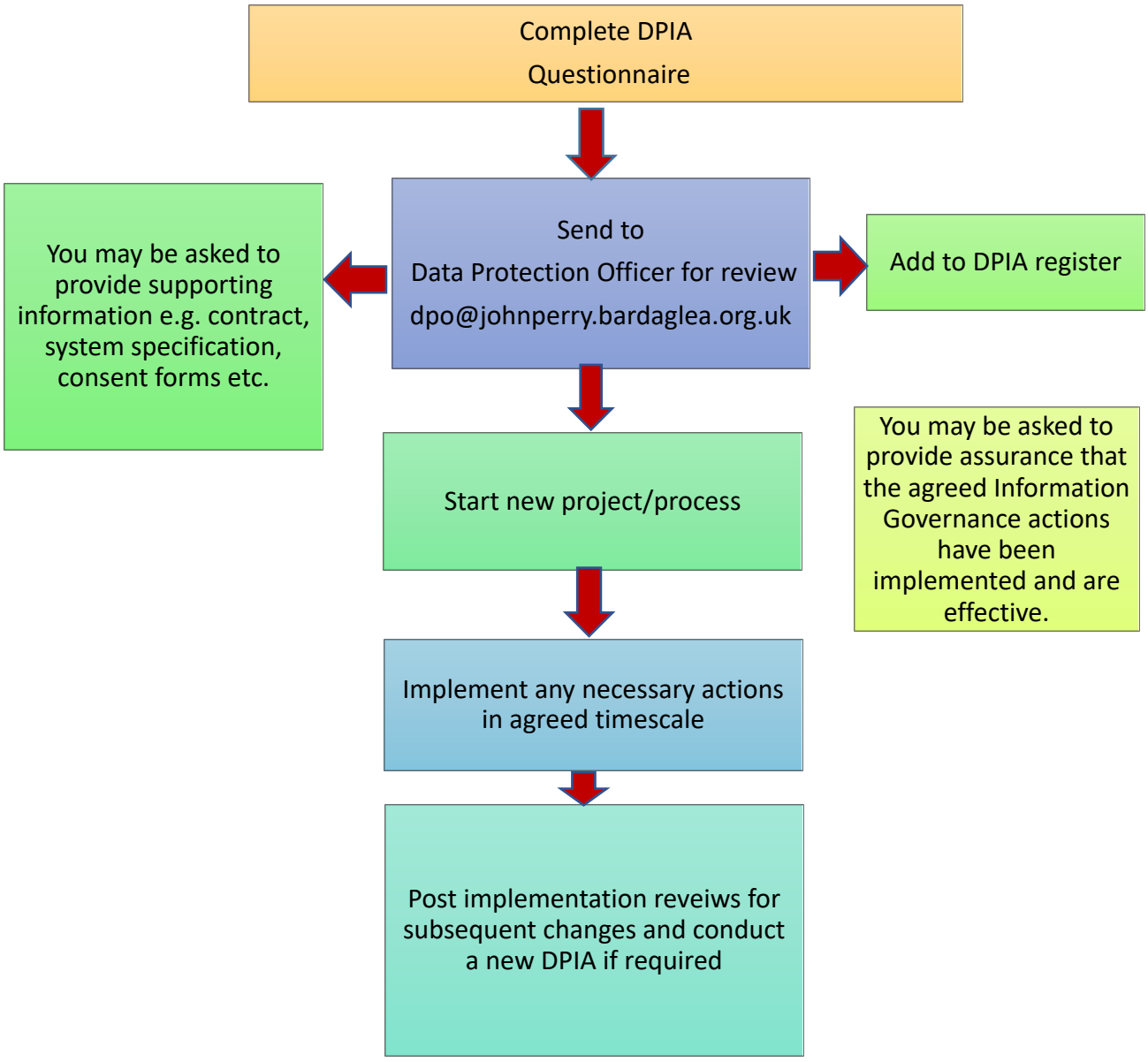


When deciding whether a DPIA questionnaire is required, if the first answer is 'yes', but the second response is 'unsure', please complete the questions in section 1 of the DPIA questionnaire to assist the decision.

If a full DPIA is required where the new process or change of use of Personal Confidential Data/Business Sensitive data, then the completed DPIA must be sent to the Data Protection Officer for review.

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. In some projects, the DPIA can be complicated. In these cases, further guidance should be sought from the Data Protection Officer.

If a high risk is identified that cannot be mitigated, then the Data Protection Officer will consult with the ICO before starting the processing. The ICO 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 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

POLICY REVIEW

This Data Protection Impact Assessment Policy will be reviewed annually by the DPO.

8. STATEMENT OF EVIDENCE/REFERENCES

The legislation and national guidance relevant to this procedure:

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

9. IMPLEMENTATION AND DISSEMINATION OF DOCUMENT

Following ratification, the Data Protection Impact Assessment Procedure will be:

- uploaded onto the School intranet and the document location confirmed to all staff
- the Data Protection Officer will provide training sessions where necessary

10. APPENDICES

Annex 1	Privacy Impact Assessment Screening Questions
Annex 2	Privacy Impact Assessment Questionnaire
Annex 3	Equality and Equity Impact Assessment

Annex one

Privacy impact assessment screening questions

These questions are intended to help you decide whether a PIA is necessary. Answering 'yes' to any of these questions is an indication that a PIA would be a useful exercise. You can expand on your answers as the project develops if you need to.

You can adapt these questions to develop a screening method that fits more closely with the types of project you are likely to assess.

You should start to fill out the template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

You **MUST** send this to your school DPO when you have completed as much as you can. Please email info@dpenterprise.co.uk

Privacy Impact Assessment Screening Questions

	Yes	No
Will the project involve the collection of new information about individuals?		
Will the project compel individuals to provide information about themselves?		
Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?		
Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?		
Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.		
Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them?		
Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private.		
Will the project require you to contact individuals in ways that they may find intrusive?		

Annex two

Privacy impact assessment template

Submitting controller details

Name of controller	
Subject/title of DPO	
Name of controller contact /DPO (delete as appropriate)	

Step 1: Identify the need for a DPIA

Explain broadly what the project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data Minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated reduced accepted	Low medium high	Yes/no

Step 7: Sign off and record outcomes

Item	Name/position/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA

Annex three
Linking the DPIA to the GDPR principles

Answering these questions during the DPIA process will help you to identify where there is a risk that the project will fail to comply with the GDPR or other relevant legislation, for example the Human Rights Act.

Article 5 Principle 1

Personal data shall be processed fairly, lawfully and in a transparent manner

Have you identified the purpose of the project?

How will you tell individuals about the use of their personal data?

Do you need to amend your privacy notices?

Have you established which conditions for processing apply?

If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?

If your school is subject to the Human Rights Act, you also need to consider:

Will your actions interfere with the right to privacy under Article 8?

Have you identified the social need and aims of the project?

Are your actions a proportionate response to the social need?

Article 5 Principle 2

Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

Does your project plan cover all of the purposes for processing personal data?

Have you identified potential new purposes as the scope of the project expands?

Article 5 Principle 3

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Is the quality of the information good enough for the purposes it is used?

Which personal data could you not use, without compromising the needs of the project?

Article 5 Principle 4

Personal data shall be accurate and, where necessary, kept up to date.

If you are procuring new software does it allow you to amend data when necessary?

How are you ensuring that personal data obtained from individuals or other organisations is accurate?

Article 5 Principle 5

Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to the implementation of appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

What retention periods are suitable for the personal data you will be processing?

Are you procuring software that will allow you to delete information in line with your retention periods?

Article 5 Principle 6

Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Will the systems you are putting in place allow you to respond to subject access requests more easily?

If the project involves marketing, have you got a procedure for individuals to opt out of their information being used for that purpose?

Do any new systems provide protection against the security risks you have identified?

What training and instructions are necessary to ensure that staff know how to operate a new system securely?