

Data Protection Impact Assessment

This document was created to help Schools complete Data Protection Impact Assessments for new systems or projects. DPIAs should be completed during the planning stage of the new project.

Where some terminology may be unclear, links to useful definitions and resources have been included.

If you have any queries about this document or Data Protection Impact Assessments you can contact the School's DPO Team at Global Policing Limited, the contact details for which are: email - data@globalpolicing.co.uk web – www.globalpolicing.co.uk/data or alternatively Tel: 0161 212 1681.

You may wish to consider the [ICO's guidance on DPIAs](#) before completing the document.

Date	
Name of product or system	
Name/s and position of staff members completing DPIA	



Brownlow
Fold Primary

Together we fly

Part 1: Why is a DPIA Required?

It is important to outline why a Data Protection Impact Assessment is being completed. Consider the following:

- What is the intended benefits of the processing for the School and individuals?
- What is the purpose of the project or new system?
- What sort of data will be processed? (e.g. data relating to children, CCTV recordings, [special category data](#))



Brownlow
Fold Primary

Together we fly

Part 2: The Processing

Scope of personal data processed – You must provide information about what data is involved in the processing. Consider the following:

- What personal data is processed, does this include [special category data](#)?
- How many individuals' personal data will be processed?
- How long will the new system retain the data for? (It may be useful to check any documentation you have been provided with, e.g. privacy notice, contract)

Type & context of processing – You must provide details of how the processing will take place. Consider the following:

- How is the personal data collected? Are you using data from a pre-existing source (e.g. SIMS) collected from individuals etc?
- Will the data be shared with any third parties?
- How is the data stored? Is cloud storage involved, is data held locally in paper copies?
- If the processing involves pupil data, have the parents/pupils been informed of this? Would they reasonably expect data to be used in this way?
- How much control do individuals have over the data? Are parents/pupils able to opt out of the system?
- If the processing involves a third party, what assurances have they provided the School? (see privacy notice or contract)

Part 3 - Consultation

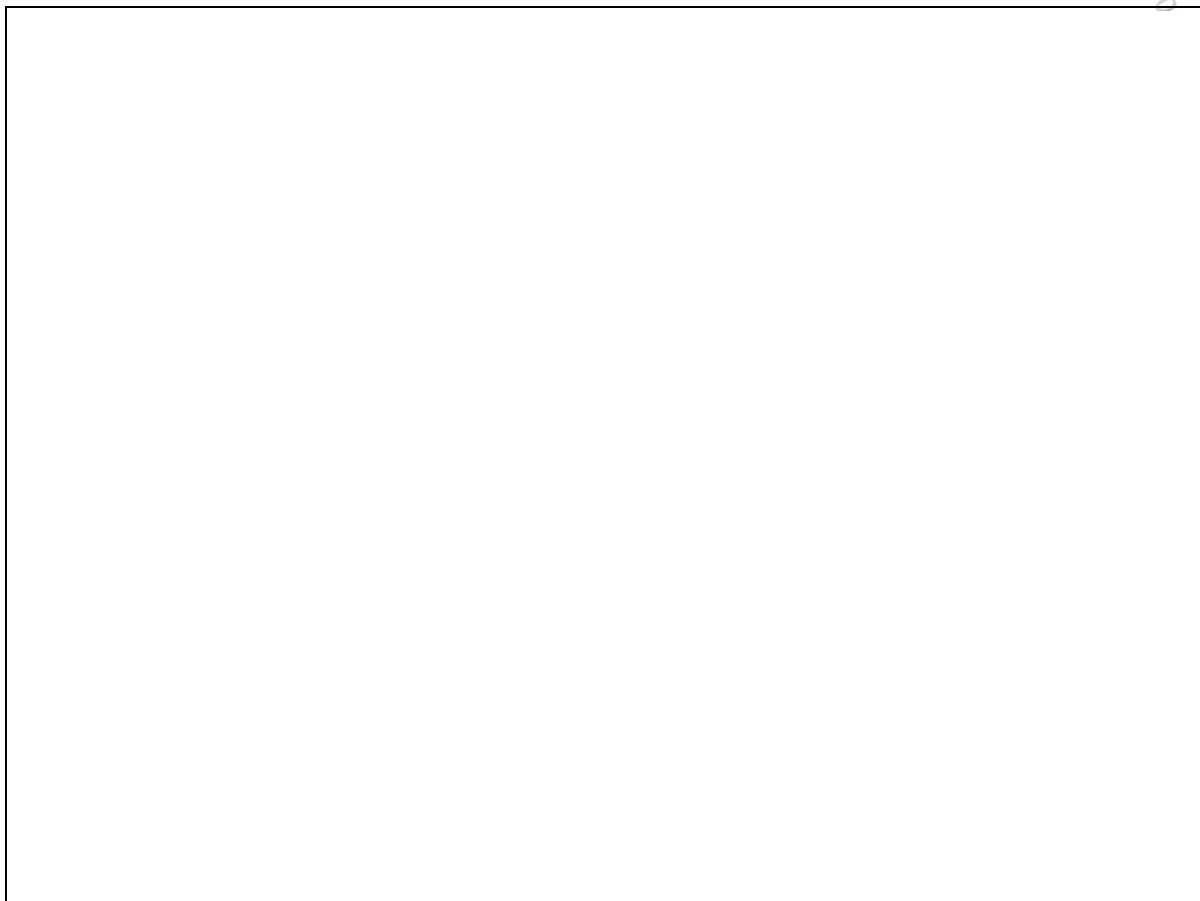
Explain whether any third parties have been consulted prior to the processing. Consider the following:

- Have you consulted with other schools who have already undertaken this processing?
- Have you asked for the views of parents or staff members? If so what was the response?
- Have you consulted with any other third parties about the processing?
- If you have not done any of the above, will it be necessary to do so or is this disproportionate?

Part 4 – Ensuring Compliance

Explain how you will ensure that the processing complies with the data protection legislation. Consider the following:

- What is your [lawful basis](#) for the processing? If you aren't sure, you can use this [interactive tool](#) to help.
- Are there any alternative ways to achieve your aim? If you already have a system which serves the same function, why is the new system an improvement?
- Are there any written assurances in place with third party data processors e.g. data sharing agreement or written contract?
- Has the third party provided a privacy notice?
- How will you ensure that any new functions which become available after the DPIA has been completed are accounted for? (The DPIA should be kept under review)
- Can you ensure that individuals are able to exercise [their rights](#) over any personal data processed in this way?
- Are there any [international transfers](#) of data? Processors may use data centres based outside of the EEA, check the privacy notice if you have been provided with one.



Part 5 – Identifying Risks

You must identify any risks that are created by this processing and what the overall risk the system presents is. We have created a guide which you can use to identify the severity of each risk.

You must first identify the likelihood of the risk causing harm as either probable (3), possible (2) or remote (1). Then you must identify the severity of the harm that can be caused as either high (3) medium (2) or low (1). These two values can then be multiplied together to identify the overall risk as outlined in this table below.

Likelihood of harm

Probable

3

3	3	6	9
2	2	4	6

Possible

2



Low	1-2	Consider some simple measures to reduce risk.
Medium	3-4	Consider possible options to reduce or eliminate risk. Careful consideration should be taken before implementing a system with medium residual risk.
High	6-9	Consider all possible options of reducing risk, high risk projects or systems should not be implemented where these risks cannot be eliminated.

Example

You may identify that the system presents a risk that child protection data is disclosed to a third party in error. You identify that the chance of this occurring is 'possible' but that due to the nature of the data the severity of harm would be 'high'. You identify that you can restrict access to the system to a small number of senior staff members and that the data can be [pseudonymised](#). This brings the likelihood and severity of harm down and changes the overall risk to low.

Describe the risk you have identified (e.g. unauthorised access to service provider's server)		Likelihood of Harm	Severity of Harm	Overall Risk
1		Choose an item.	Choose an item.	Choose an item.
2		Choose an item.	Choose an item.	Choose an item.
3		Choose an item.	Choose an item.	Choose an item.
4		Choose an item.	Choose an item.	Choose an item.

5		Choose an item.	Choose an item.	Choose an item.
6		Choose an item.	Choose an item.	Choose an item.

Now you must identify what steps you can take to reduce the risks and whether there is any risk remaining after this. These steps should be approved by a senior member of staff.

Risk	Steps to reduce risk	Effect on risk	Remaining Risk	Approved
1		Choose an item.	Choose an item.	Choose an item.
2		Choose an item.	Choose an item.	Choose an item.
3		Choose an item.	Choose an item.	Choose an item.
4		Choose an item.	Choose an item.	Choose an item.
5		Choose an item.	Choose an item.	Choose an item.
6		Choose an item.	Choose an item.	Choose an item.

The outcome of the DPIA should be signed off by a senior member of staff such as the School Business Manager or Head Teacher. If there is any remaining risk then a senior member of staff must sign to indicate that these risks are accepted.

You must [consult with the ICO](#) before proceeding with processing which involves high risk which you are unable to reduce always ask for the advice of the DPO before doing this. The School's DPO should be asked to provide feedback on the DPIA.

Part 7 – Sign Off

Measures Approved By: Name/ Position/ Date	
Remaining Risk Approved By:	
DPO Advice:	
DPO Name/ Date	