BHJS Bromley Heath Junior School

Introduction

This template can be used to record any data protection impact assessments (DPIAs) undertaken. It is based on the Information Commissioner's Office (ICO) example template and follows the process set out in the ICO's guidance.

A DPIA must be carried out for any processing of personal data that is considered high risk. A DPIA should also be undertaken at the start of any major project involving the use of personal data, or if significant changes are being made to an existing process.

There is a SchoolsDPO 'DPIA Need Identifier' available to help decide whether to undertake a DPIA. There is also a risk assessment methodology to help assess the level of risk. They can both be found in the Data Protection Impact Assessment folder under Key Resources on the Data Protection Lead network.

Document Control

Version	Date	Author	Summary of Changes	Approver	Approval Date

Step 1: Summary of Initiative/Project	
Describe the scope of the initiative/project e.g. aims and objectives, business/educational case, duration, reach, visibility outside school/trust	
Status of Initiative/Project Describe the current phase of development /implementation of the initiative/project. If the DPIA is retrospective describe why it is being carried out	
Step 2: Description of the processing	
Nature of the processing	
Method(s) of collection e.g. online or paper-based forms completed by data subjects or from other sources	
Source(s) of the personal data being processed if from third party sources describe them	
Processing activities - how will data be used (processed) after collection?	
Scope of data sharing with third parties (you may want to refer to a flow diagram)	

Scope of the processing	
Categories of personal data - identify each category of personal data processed to include any special category data and information relating to criminal convictions and offences	
Categories of data subject e.g. pupils, parents, staff, volunteers, governors, visitors, contractors	
Format of the personal data e.g. paper records, electronic documents, management information systems, online 'cloud' files etc	
Storage location e.g. school-based servers, trust-based servers, cloud-hosted services in UK, EEA or elsewhere, locked filing cabinets	
Duration and frequency of processing in relation to nature of the initiative or relationship with the data subject	
Volume of data subjects and records - this can be approximate if it is difficult to be precise a the time of the DPIA	
Retention periods for personal data - how long will the personal be retained for the processing purposes?	

Will there be differing retention periods for different categories of personal data or data subject?	
Context of the processing	
Relationship with the data subjects - describe the nature of the school's relationship with the data subjects	
Data subjects expectations - how much control will they have? Would they consider this to be a reasonable use of their personal data?	
Relevant matters of public concern - are there any issues of public concern relating to the scope of the processing that should be taken into account?	
Purposes of processing	
Benefits to the data subject - describe how the processing benefits the data subjects/individuals directly or indirectly	
Benefits to the school/trust - describe how the processing benefits the school/trust either directly or indirectly	
Benefits to third parties - describe how the processing benefits any third parties either directly or indirectly	

Step 3: Consultation process	
Input of school/trust professionals /stakeholders e.g. advice from staff, subject experts, Trust DPO, HR Team etc as appropriate	
Input from data subjects or their representatives - describe views sought, methods used as relevant; or justification for not seeking input	
Input of any relevant third parties e.g. wider school/trust community, third party processors, processors, facility hirers, lawyers etc as appropriate; or justification for not seeking input	
Step 4: Assessment of necessity and proportionality	
Purpose and necessity - describe how the processing will achieve the purpose of the initiative/project. Why is it necessary?	
Lawful basis for processing - identify the most approprie lawful basis for processing. Identify a lawful condition for the processing of any special category data of criminal convictions data as appropriate (see Guidance on Lawful Basis for more advice and guidance in choosing a lawful basis).	
Fairness and transparency - describe how data subjects will be informed about the processing of their personal data, e.g. through privacy notices, newsletters, consent forms etc.	

Data quality and minimisation - describe how the data will be kept accurate and up to date. Describe the steps that will be taken to ensure only the minimum amount of personal data that is necessary is collected and used. How will you prevent the data being used for purposes beyond the scope of the initiative/project?	
Storage limitation - describe how the personal data will not be retained longer than necessary for the purposes of the processing.	
Security, integrity and confidentiality - describe the measures that will be in place to keep the personal data secure, including protection against personal data breaches e.g. physical, technical and organisational measures.	
Data subject rights - describe how data subjects will be able to exercise their rights: to be informed, access their personal information, rectification, erasure, objection. (this is about clear information in your privacy notices and how you make them available to data subjects and how you remind them, as appropriate.	
Third party processors - where relevant, describe how you will check that any third party processors will keep the personal data secure and how they are compliant with data protection law.	
International transfers of personal data - How will you ensure the international transfer rules are met in relation to any transfers of personal data beyond the UK?	

N.B. There is an adequacy agreement in place between the UK and EEA countries which means that these requirements are met. For any other countries, seek the advice of the DPO.	

Step 5: Identification and assessment of risk (see risk assessment matrix and examples of risk)				
Ref No.	**Source of risk and potential impact on data subjects or associated school/trust risks**	**Likelihood of harm**	**Impact/severity of harm**	**Overall risk** Low, medium, high
1				
2				
3				
4				

Step 6: Identification of controls and measures to reduce risk				
Ref No.	**Controls or measures to reduce or eliminate risk**	**Effect on risk** - extent to which risk is eliminated, reduced, accepted	**Residual risk** - low, medium, high	**Measure approved** Yes/No
1				
2				
3				
4				

	Name/position/date	Notes
Measures approved by		Integrate any actions back into project plan with timeline and responsibility for completion
Residual risks approved by		If accepting any residual high risk contact the DPO who will consult with the ICO
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
Any comments		
Consultation responses reviewed by:		If your decision departs from consultation views, you must explain your reasons
Comments		
This DPIA will be kept under review bi-annually by the Head Teacher		