[SCHOOL]
POLICY FOR DATA PROTECTION IMPACT ASSESSMENTS

1 POLICY OBJECTIVES

The General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA) aim to protect the rights of individuals about whom data is obtained, stored, processed or supplied. A key principle is that data controllers should assess and mitigate the risks of any new data processing activity. A Data Protection Impact Assessment (DPIA) is a process to help identify and minimise the data protection risks of a project.

2 SCOPE

[SCHOOL] must undertake a DPIA for any processing that is likely to result in a **high risk** to individuals. This includes some specified types of processing. The School will use the Information Commissioners Office (ICO) screening checklists to help decide when to undertake a DPIA.

In line with best practice guidance, the School will undertake a DPIA for any other **major project** that requires the processing of personal data.

3 AWARENESS

The School provide training so that **all staff** understand the need to consider a DPIA at the early stages of any plan involving personal data.

We will review relevant policies, processes and procedures to include references to DPIA requirements.

The School provides training for relevant staff on how to carry out a DPIA.

3 UNDERTAKING A DPIA

The School uses the ICO screening checklist in Annex 1 to identify the need for a DPIA, where necessary.

When drawing up a DPIA the School will:

- describe the nature, scope, context and purposes of the processing;
- assess necessity, proportionality and compliance measures;
- identify and assess risks to individuals; and
- identify any additional measures to mitigate those risks.

The School will consider how best to consult individuals and other relevant stakeholders. Their views will help the School to check that the processing is necessary for and proportionate to our purposes, and will ensure compliance with data protection principles.

To make an objective assessment of the level of risk, the School will consider both the likelihood and the severity of any impact on individuals. High risk could result from either a high probability of some harm, or a lower possibility of serious harm. The School will identify measures to eliminate or reduce high risks.

The School will consult our Data Protection Officer (DPO) and, where appropriate, individuals and relevant experts, including any processors who may be involved. The views of data processors will help the School understand and document their processing activities and identify any associated risks.

The School will use the ICO DPIA template in Annex 2 to record our decision-making, including any difference of opinion with our DPO or individuals consulted.

If the School identifies a high risk that cannot be mitigated, we will consult the ICO before starting the processing. The ICO will give written advice within eight weeks, or 14 weeks in complex cases. If appropriate, the ICO may issue a formal warning not to process the data, or ban the processing altogether.

4 IMPLEMENTING THE DPIA

The School will implement the measures identified in the DPIA, and integrate them into the project plan.

DPIAs will be kept under review and revisited when necessary.

ANNEX 1
ICO SCREENING CHECKLIST

We consider carrying out a DPIA in any major project involving the use of personal data.

We consider whether to do a DPIA if we plan to carry out any other:

- evaluation or scoring;
- automated decision-making with significant effects;
- systematic monitoring;
- processing of sensitive data or data of a highly personal nature;
- processing on a large scale;
- processing of data concerning vulnerable data subjects;
- innovative technological or organisational solutions;
- processing that involves preventing data subjects from exercising a right or using a service or contract.

We always carry out a DPIA if we plan 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 a publicly accessible place on a large scale;
- use innovative technology in combination with any of the criteria in the European guidelines;
- use profiling, automated decision-making or special category data to help make decisions on someone's access to a service, opportunity or benefit;
- carry out profiling on a large scale;
- process biometric or genetic data in combination with any of the criteria in the European guidelines;
- combine, compare or match data from multiple sources;
- process personal data without providing a privacy notice directly to the individual in combination with any of the criteria in the European guidelines;
- process personal data in a way that involves tracking individuals' online or offline location or behaviour, in combination with any of the criteria in the European guidelines;
- 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.

We carry out a new DPIA if there is a change to the nature, scope, context or purposes of our processing.

If we decide not to carry out a DPIA, we document our reasons.

ANNEX 2
ICO DPIA TEMPLATE

[SCHOOL]

DPIA for [PROJECT] – [DATE]

This Data Protection Impact Assessment (DPIA) has been based on the template provided by the Information Commissioner's Office (ICO). It follows the process set out in the ICO's DPIA guidance and reflects the 'Criteria for an acceptable DPIA' set out in European guidelines.

Data Controller details

Name of controller	
Name of advising DPO	
Name of controller DPO	
Name of controller contact	

Step 1: The need for a DPIA

1. Project Aims 2. Type of processing involved 3. Factors indicating the need for a DPIA
1. 2. 3. Factors in ICO's 'DPIA screening checklist' relevant in whole or part: Additional factors:

Step 2: Description of the processing

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?

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?

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)?

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: 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?

Step 5: Identification and assessment of risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm** (Remote, Possible, Probable)	**Severity of harm** (Minimal, Significant, Severe)	**Overall risk** (Low, Medium, High)

Step 6: Identification of 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** (Eliminated, Reduced, Accepted)	**Residual risk** (Low, Medium, High)	**Measure approved** (Yes/No)

Step 7: Sign off and record of outcomes

Item	Name/position/date	Notes
Measures approved by: Date:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by: Date:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided by: Date:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by: Date:		If overruled, you must explain your reasons
Comments: DPO advice accepted in full		
Consultation responses reviewed by: Date:		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