Data Protection Impact Assessment (DPIA) procedure

Reviewed:	January 2025
Adopted by Governors:	Full Governing Body 23rd June 2022
Next review:	Spring 2027

Kings Mill School & Residence

1. Scope

All projects/changes that involve processing personal data, or any activities (both internal and external) that affect the processing of personal data and impact the privacy of data subjects, are within the scope of this procedure and will be subject to a Data Protection Impact Assessment (DPIA).

The School requires the DPIA process to be carried out on projects/changes involving personal data to help ensure compliance with data protection legislation and embed 'privacy by design'.

2. Responsibilities

The School's Data Protection Officer (DPO) is responsible for performing the necessary checks on personal data to establish the need for conducting a DPIA. The DPO, with assistance from relevant managers such as the School Business Manager (SBM) will maintain a record of all DPIAs, the corporate DPIA log.

The Head Teacher as the Information Asset Owner (IAO) is responsible for implementing any privacy risk solutions identified and the DPO, along with the Senior Leadership Team are responsible for ensuring that any decisions made are in line with this procedure and the School's Data Protection Policy.

The IAO and the DPO are responsible for ensuring appropriate controls are implemented to mitigate any risks identified as part of the DPIA process and the subsequent decision to proceed with the processing.

Employees, specifically School Business Managers, Senior IT Staff (ICT) and the IAO are responsible for identifying the need for a DPIA. A DPIA should be carried out at the start of a project/change to the way personal data is used, or as soon as it becomes evident that one needs to be undertaken.

Non- compliance with this procedure can lead to fines imposed by the Information Commissioners Office (ICO).

3. Carrying out a DPIA

A DPIA is designed to describe the processing, assess the necessity and proportionality of processing and help manage the risks to rights and freedoms.

A DPIA should be carried out as soon as possible and ideally prior to any processing taking place.

A DPIA can be done on a single processing operation or a set of similar operations. This means it can be used to assess multiple projects, for example a new technology used to collect data in a similar way across different services.

However, this does not mean that it is mandatory for all processing operations; a DPIA is only mandatory if the processing is *'likely to result in high risk to the rights and freedoms of natural persons'.* If it is unclear whether or not a DPIA is required based on this criteria, then a DPIA should be carried out nonetheless.

Due to their inherent risks the following processing operations will always be considered *'likely to result in high risk':*

- Large Scale Use of Sensitive Data - processing on a large scale of special category data, or of personal data relating to criminal convictions and offences.
- Public Monitoring (CCTV) - systematic monitoring of a publicly accessible area on a large scale
- New Technologies - processing involving the use of new technologies, or the novel application of existing technologies (including Artificial Intelligence).
- Denial of Services - Decisions about an individual's access to a product, service, opportunity or benefit which is based to any extent on automated decision-making (including profiling) or involves the processing of special category data.
- Large Scale Profiling - any profiling of individuals on a large scale
- Biometrics - any processing of biometric data.
- Genetic Data - any processing of genetic data other than that processed by an individual GP or health professional, for the provision of health care direct to the data subject.
- Data Matching - combining, comparing or matching personal data obtained from multiple sources.
- Invisible Processing - processing of personal data that has not been obtained direct from the data subject in circumstances where the controller considers providing information to the data subject as required by Article 14 (identity of the controller, categories of personal data collected, rights of the data subject etc.) would prove impossible or involve disproportionate effort.
- Tracking - processing which involves tracking an individual's geolocation or behaviour, including but not limited to the online environment.
- Targeting of Children or other Vulnerable Individuals - The use of the personal data of children or other vulnerable individuals for marketing purposes, profiling or other automated decision-making, or if you intend to offer online services directly to children.
- Risk of Physical Harm - Where the processing is of such a nature that a personal data breach could jeopardise the physical health or safety of individuals.

As part of the School's commitment to 'privacy by design', it will consider processing operations already underway under this procedure. Just because a process is underway, does not mean that the risk to privacy/personal data cannot change.

4. The Process

The DPIA can be done at various levels as long as it captures the key elements of a DPIA. These are:

- Screening questions (Stage 1)
- Describe the processing (Stage 2)
- Consider consultation
- Assess necessity and proportionality
- Identify and assess risks
- Identify measures to mitigate the risks
- Sign off/approval and record outcomes Integrate outcomes into a project plan
- Keep your DPIA under review

The detail required will depend on the level of privacy risk posed by the proposed project/ change to the way personal data is used. The level of risk is assessed at Stage one. The various stages are outlined in more detail below.

Stage 1 – To decide if a DPIA is needed, staff should complete the Stage 1 form, which consists of screening questions to help establish if a full DPIA is required. Once completed, staff should email it to kingsmill.specialschool@eastriding.gov.uk. This will be logged and a decision made by the SBM or DPO as to what follow up work needs to be carried out. Any processing activities which are already specified as not requiring a DPIA will be filtered out at this stage.

Any conversation with the DPO or School Business Manager as a result of Stage one of this procedure will be recorded. This will help the School meet its commitment to privacy by design and demonstrate what action is taken and why. The IAO will be copied in to all DPIA stage one responses and notified that the DPIA will be raised at a meeting with the DPO.

Stage 2 – Following Stage one, further work may be required and this should be done using Stage 2 form. This is normally the case if any of the answers to the screening questions are 'yes', although a DPIA can take place regardless of any high risk processing. The DPO and School Business Manager is responsible for deciding what type of assessment is required for each project/change to the way personal data is used in line with this procedure. The IAO will be copied in to all DPIA Stage two responses.

Stage 2 is designed to ensure that the School can meet its obligations. It is possible to do this without using the template, however a record must be created on the DPIA log and all points of this procedure still considered.

Once Stage two of the DPIA has been completed it will be sent to the next convenient meeting with the DPO to be discussed and approved, or if urgency is required, it may be circulated virtually for consideration.

Once completed the DPIA should inform all aspects of the project/change, thus ensuring the School remains compliant with data protection legislation. Privacy risks and their solutions should be continually monitored and the DPO is responsible for ensuring solutions to risks are implemented and for escalating DPIAs to the ICO if required (see section 6). Once complete, the DPO should ensure DPIAs are reviewed on a regular basis.

The School will publish a summary of all Stage two DPIAs on the School's website.

5. Prior Consultation

Where the DPIA identifies that processing of personal data will result in *'high risk'* to the data subject and in the absence of risk mitigating measures and controls, the School will consult with the ICO. The DPO will advise whether or not the DPIA should be sent to the ICO and this will be communicated to the IAO.

6. Evaluation

This procedure will be reviewed/updated by the school on a biennial basis to ensure the content remains current.

7. References

Data Protection Policy

Record of review/amendment

Review Date:	January 2025	**Page No (Other info):**	
Original:	No amendments required		
Amendment:			

Review Date:		**Page No (Other info):**	
Original:			
Amendment:			

Review Date:		**Page No (Other info):**	
Original:			
Amendment:			