Data Protection Impact Assessment (DPIA) Policy and Procedure

1. Introduction

1.1 Data Protection Impact Assessments (DPIA) (also known as Privacy Impact Assessments PIA)) are an integral part of taking a 'privacy by design' approach.

1.2 A DPIA is a process which minimises the privacy risks of new projects or work activities by considering the impact that the proposed project or activities will have on the individuals involved to ensure that the potential problems are identified at the outset.

1.3 This policy and procedure is based on comprehensive guidance produced by the Information Commissioner's Office, which can be accessed at:

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

1.4 It has also been developed to meet requirements of the UK General Data Protection Regulation (UK GDPR)

2. When is a DPIA required?

2.1 The Trust is obliged to carry out a DPIA whenever it is implementing a new (or making a change to an existing) process, system, project, or work activity that could have an impact on the privacy of individuals.

3. Stages of a DPIA

3.1 Stage 1 – the initial screenings questions

3.1.1 This section is to be completed by the staff member or project lead responsible for delivering the proposed change in liaison with the designated school data protection contact. The purpose of the screening questions (Appendix A) is to assess whether a full DPIA is required and ensure that the investment in the Trust is proportionate to the risks involved.

3.1.2 If the answers to the questions are 'no', the screening process has not identified any DPIA concerns and the process is complete.

3.1.3 If response to any of the questions is 'yes', then an initial DPIA must be undertaken.

3.1.4 It is important to get this stage right. If the Trust is challenged by the Information Commissioner's Office a decision about why a DPIA was or wasn't undertaken must be defendable.

3.2 Stage 2 – Data Protection Impact Assessment

3.2.1 The responses to the screening questions will give an indication as to the appropriate scale of the DPIA. In some cases, the answers to the screening questions may not be known and the process will need to be re-visited when more information comes to light.

3.2.2 The DPIA must be completed by the staff member or project lead responsible for delivering the proposed change, with the assistance of the designated school data protection contact who will liaise with the Data Protection Officer to complete the appropriate DPIA form.

3.2.1 There are three possible outcomes to the initial DPIA:

- The initial DPIA is incomplete and will have to be repeated or further information obtained;
- The initial DPIA is complete and no privacy risks have been identified;
- The initial DPIA has identified a privacy risk.

3.3 Stage 3 – identifying compliance risks

3.3.1 Identifying compliance risks will be necessary where there are any significant information governance risks identified. The DPO with the designated school data protection contact will review the checklist of Data Protection Principles in order for each principle to be considered.

3.3.2 The DPIA will identify how any identified risks will be mitigated. This will include identified issues, associated actions, related roles and responsibilities, and timescales.

4. Measures to reduce the risk

4.1 It is important to remember that the aim of a DPIA is not to completely eliminate the impact on privacy. The purpose of the DPIA is to reduce the impact to an acceptable level while still allowing a useful project to be implemented.

4.2 Examples of measures:

- Obtaining the data subject's consent;
- Deciding not to collect or store particular types of information;
- Devising retention periods which only keep information for as long as necessary and planning secure destruction of information;
- Implementing appropriate technological and organisational security measures;
- Ensuring that staff are properly trained and are aware of potential privacy risks;

- Developing ways to safely anonymise the information, when it is possible to do so;
- Producing guidance for staff on how to use new systems and how to share data if appropriate;
- Using systems which allow individuals to access their information more easily and make it simpler to respond to subject access requests;
- Taking steps to ensure that individuals are fully aware of how their information is used and can contact the Trust for assistance if necessary;
- Selecting data processors who will provide a greater degree of security and ensuring that agreements are in place to protect the information which is processed on the Trust's behalf;
- Producing data sharing agreements which make clear what information will be shared, how it will be shared and with whom it will be shared.

5. Integrating DPIA outcomes into the project plan

5.1 The DPIA findings and actions should be integrated with the project plan. The person responsible for the DPIA and the overall project should ensure that the steps recommended are implemented and return to the DPIA at various stages of the project's development and implementation. Large projects are more likely to benefit from a more formal review process.

5.2 If the DPIA generates actions that will continue after the assessment has finished, the person responsible should ensure that these are monitored and that all lessons learned from the DPIA are recorded for future projects.

APPENDIX A

DATA PROTECTION IMPACT ASSESSMENT (DPIA) INITIAL SCREENING FORM

Project name:	
Brief outline of the project:	
Project lead:	
Project dates (from – to):	

SECTION 1: DPIA screening questions

These questions are intended to help the Trust decide whether the DPIA is necessary. Answering 'yes' to any of these questions is an indication that a DPIA would be a useful exercise.

Once completed please forward to the Data Protection Officer for review.

Question	Yes (✓)	No (✓)	Notes
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 which it is not currently used, or in a way not currently used?			
Does the project involve you using new technology which 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 which can have a significant impact on them?			
Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? This might include, for example, health records, criminal records, or other information that people would consider to be particularly private.			
Will the project require you to contact individuals in ways which they may find intrusive?			

SECTION 2: Data Protection Officer (DPO) feedback/decision
