DATA IMPACT ASSESSMENT POLICY

SPRING TERM 2025

DUE FOR RENEWAL: SPRING TERM 2027

CHANGES

November 2020	Policy implemented

CONTENTS

1. INTRODUCTION

Completion of a Data Protection Impact Assessment (DPIA) is a requirement of Article 35 of the General Data Protection Regulation (GDPR).

The Trust needs to collect and process a wide variety of information in respect of its Trustee's, employees, pupils, suppliers and visitors. However, we are committed to processing all personal information in accordance with the General Data Protection Regulation, UK Data Protection Act 2018 (DPA 2018) and any other codes of conduct.

Completion of a DPIA will help us to identify and minimise our privacy risks, to comply with our data protection obligations and meet individuals' expectations of privacy.

2. SCOPE OF POLICY

The policy covers any project that will change the way we collect or use personal information. That can be a change to an existing process or policy or a new IT system, technology or procurement activity. For the purposes of this policy 'project' will cover all of the activity listed above. The type of relevant activity are listed below, these are examples only and not an exhaustive list.

- A new database storing and accessing personal data
- A new data processing technology is being introduced
- A proposal to identify people in a particular group or demographic and initiate a course of action (e.g. identifying students believed to be at risk)
- A new surveillance system such as CCTV
- A new provider for HR services
- Where it is not clear whether a DPIA is required
- Any system based on automated processing, including profiling or automated decision making
- Processing of sensitive data or data of a highly personal nature, including special categories of data as defined by GDPR or considered sensitive in Trusts
- Data concerning vulnerable data subjects

This policy provides a process which will enable:

- identification of the need to complete a DPIA through a set of screening questions, taking into account among others the risks of varying likelihood and severity for the rights and freedoms of natural persons
- the collection of sufficient information about a project to complete a DPIA
- privacy risks identified by the DPIA to be documented and considered

The process should be followed from the start of a project to ensure that potential problems are identified at an early stage. This will ensure that we can address issues early:

- before we have invested extensive time and costs into the project
- before we have caused any damage to our reputation
- before we have incurred associate costs to risks not being managed
- when the information can influence the direction of project

Although the policy sets out our legal requirements for DPIA's in respect of new projects, information asset owners:

- may wish to use it as a tool to review existing arrangements if they consider there to be privacy risks
- Remain responsible for implementing measures to appropriately manage risks for the rights and freedoms of data subjects, even where an obligation to carry out a DPIA has not been met
- Must continuously asses the risk created by their processing activities

3.0 OUR TRUST'S ROLES AND RESPONSIBILITIES

3.1 Board of Trustees

This policy must be complied with fully by the Board of Trustees and staff who are data asset owners and/or who are authorised to initiate a project to make changes to the way we process personal data or implement a new IT system, technology or procurement activity.

Employees who do not comply with this policy may face disciplinary action.

3.2 Data Protection Officer

The data protection officer should be notified as soon as the Trust intends to commence a project that may affect the privacy of individuals' personal data.

The data protection officer will support the Trust to assess the project to determine if a full DPIA is required and will assist the Trust in its completion.

4.0 DEFINITIONS

4.1 The following table provides a list of important terms and their meanings for the purposes of this data protection impact assessment policy.

TERM	DESCRIPTION
Project	Any project that will change the way we collect or use personal information. That can be a change to an existing process or policy or a new IT system, technology or procurement activity.
Privacy Information	Our purpose for processing personal data, our retention periods for that personal data and who it will be shared with.
Data Protection Impact Assessment (DPIA)	A tool that can help us to systematically and comprehensively analyse our processing and help us identify the most effective way to comply with our data protection obligations, minimise data protection risks and meet individuals' expectations of privacy. DPIAs are a legal requirement for processing that is likely to be high risk. But an effective DPIA can also bring broader compliance, financial and reputational benefits, helping us demonstrate accountability and building trust and engagement with individuals.
Data Subject	The identified or identifiable individual that the personal data being held or processed relates to.

Personal data	Information relating to a natural identifiable person, whether directly or indirectly.
Special category data	These are highly sensitive pieces of information about people. They are important because under GDPR they are afforded extra protection in terms of the reasons we need to have to access and process that information. This is defined as data relating to: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Health - physical or mental • Trade union membership • Sex life or sexual orientation • Data relating to criminal offences is also afforded similar special protection. In education we also apply this special protection to other categories of personal data which is considered to be highly sensitive, such as: • Free school meals • Pupil premium eligibility • Special educational needs • Children in need/children looked after • Children Services Interactions • Safeguarding
Processing	This includes anything that is done with personal data such as collecting, recording, storing, organising, structuring, adapting, altering, retrieving, using, sharing, erasing or destroying. Processing can be automated or manual.
Data asset	Data asset is information held by the Trust and is categorised based on its content or use. It could be a collection of paper or electronic records that contain customer/service user, stakeholder, staff or pupil information.

5.0 DATA PROTECTION IMPACT ASSESSMENTS

It is a requirement of GDPR that a Data Protection Impact Assessment (DPIA) is carried out in certain circumstances. This section will explain when a DPIA has to be done and how it should be carried out. The procedures in this section are designed to minimise the risk of harm that can be caused by the use or misuse of personal information by addressing data protection and privacy concerns at the design and development stage of a project.

As well as complying with the law, DPIA's can benefit the Trust in other ways, such as increasing pupil, parent and employee confidence in the way we use their personal information. A project which

has been subject to a DPIA should be less privacy intrusive and therefore less likely to affect individuals in a negative way.

5.1 When is a DPIA completed?

A DPIA should be completed at the initial phase of a project or at the point of creating a new asset or process that involves personal data. For procurement activity a DPIA should be considered prior to tender so that privacy risks are assessed when setting out the Trust's specifications and when tender responses are received.

As soon as the data asset owner (the staff member who wants to make the change or implement the new system) identifies that there may be a risk to personal data they should make contact with the Data Protection Officer. The Data Protection Officer will help determine whether a DPIA is required and support the completion of this.

5.2 How to identify the need for a DPIA

This policy requires that the Data Protection Officer is made aware of any projects that will involve the processing of personal data to assist with assessing whether a DPIA is required.

A template of the Trust's DPIA is at appendix A. Section 2 – Information Assessment, will determine whether a full DPIA is required. If we answer 'YES' to any of the screening questions in this section we will need to complete a DPIA. If all of the answers are 'NO' in this section there is no need to go on to complete the remainder of the form.

5.3 How to complete a DPIA

5.3.1 Describe the processing: We initially need to describe the processing – the Information flows section of the DPIA. This will define the type of personal data being used, where the data came from, who it is shared with and a description of the flow of data and information.

5.3.2 Consider consultation: It is important to consult with individuals and stakeholders throughout the process so that we are satisfied that the risks have been appropriately considered and addressed. This is to include individuals who will be involved in processing the personal data in the Trust, individuals based on their area of expertise, e.g. HR or IT and any external providers e.g. web based systems that will host personal data or a HR provider.

5.3.3 Identify and assess risk: consider compliance risks, but also broader risks to the rights and freedoms of individuals, including the potential for any significant social or economic disadvantage. The focus is on the potential for harm – to individuals or to society at large, whether it is physical, material or non-material.

A key aspect is identifying that any ICT system, especially a system that is accessible on the internet, has the appropriate security the address any concerns around the confidentiality, integrity and availability of the data that it is processing.

The risks to ICT systems must be considered very carefully, due to the high probability that any vulnerability will be exploited, and the difficulty in tracing any data that may be affected.

5.3.4 Assess proportionality: Once we have decided that a DPIA is required we should assess the proportionality required based on the risks identified. To assess the level of risk, a DPIA must consider both the likelihood and the severity of any impact on individuals.

5.3.5 Identify measures to mitigate risk: A DPIA does not have to indicate that all risks have been eradicated. However it will help us document them and assess how we have reduced risks and decide whether or not any remaining risks are justified.

5.3.6 Sign off and record outcomes: The DPIA should be signed off by the Data Protection Officer and the information asset owner or the Chief Executive Officer.

5.3.7 Integrate outcomes into plan: We will ensure our outcomes are included in our organisational processes and ensure the outcome influences our plans.

5.3.8 Keep under review: Our DPIA is an ongoing process that is subject to regular reviews. We will ensure that the measures we have implemented to reduce risk remain appropriate and are achieving the desired results.

5.4 Completed DPIAs

The completed screening questions and DPIA should be retained with the project documentation.

An electronic copy should be stored in the Trust's drive in a folder for Data Protection Impact Assessments.

A record that the DPIA has been completed should added to the DPIA register (see Appendix B).

6.0 OUTSTANDING RISKS

A key part of the DPIA process is deciding which risks to take forward and recording whether the risks that have been identified are to be reduced, transferred, or accepted. It may be decided that an identified risk is tolerated.

However, if there are risks which cannot be reduced, transferred, or accepted then it will be necessary to reassess the viability of the project.

In such circumstances the Trust should reject the processing and look at alternatives.

APPENDIX A: DATA PROTECTION IMPACT ASSESSMENT

OVERVIEW

This procedure provides the guidance and documentation for the completion of a Data Protection Impact Assessment (DPIA) for any programme or project being undertaken within the Trust.

The procedure consists of two parts, the first part being a set of screening questions that will determine if the next part, the system assessment has to be completed.

All projects must undertake the screening questions as a minimum so that due process can be shown to have been completed.

Service overview	
Service Name	
Purpose of service	
Overview of how the service operates	

Information assessment	**YES/NO**
Does the service process 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 new purpose or in a new way that is different from any existing use?	
Does the project involve you using new technology which might be perceived as being privacy intrusive? For example, the use of biometrics, facial recognition or location tracking.	
Is the information to be used about individuals' health and/or social wellbeing?	
Does the information contain any financial details? Including individuals or businesses	
Will the project result in personal information being aggregated?	

Information flows

The collection, use and deletion of personal data should be described here and it may also be useful to refer to a flow diagram or another way of explaining data flows.

Type of personal data being used :	
Data origin	
Data is shared with?	
Brief Description of the flow of data/information	

Legal Requirements	
Are there any legal enablers or legislation, of which you are aware, that aid in the use of personal information for the purposes you have specified in this questionnaire? If so, please specify in Further Information (below).	
Further information – Please provide any further information that will help in determining the Data Protection impact.	

DPIA outcome Does the system require further assessment for compliance?	
System assessment needed:	

Risks (Privacy / Availability / Integrity) List any identified risks to privacy and personal information of which the project is currently aware. Risks to be populated in the Risk Register.			
Risk Description **(to individuals, to the Authority or to wider compliance)**		**Proposed Risk solution (Mitigation)**	**Is the risk reduced, transferred, or accepted? Please specify / justify.**
1	Unauthorised person accesses Trust's data via system	• Assurance that identity verification is robust, with details of how it operates • Evidence that the system has been fully tested / accredited to ensure that it cannot be compromised using technical tools • Evidence of monitoring of unusual activity	
2	Data transferred to system is intercepted, accessed and / or changed by unauthorised people	• Evidence that data transfers are encrypted	
3	Authorised people retain Trust's data accessed / transferred via system longer than necessary	• Can data be downloaded from system? • Is any Information rights management applied? • Is clear guidance given to retention? • Do admin staff from supplier / partner take copies of data (eg for support purposes)	
4	Client data is retained by system supplier longer than necessary	• Do admin staff from supplier / partner take copies of data (eg for support purposes) • Evidence of information management / retention by supplier • Details of how system backups are managed	
5	System data is merged with data from other organisations	• Evidence that data segregation has been implemented	

6	System data is stored in a location that is not compatible with the data protection Act	• Evidence that data is stored in the UK	
7	Trust data is copied and archived by unauthorised third parties	• Evidence that internet archives / robots cannot copy data • Details of how system backups are managed	
8	System is used by employees for purposes other than the stated purpose	• Evidence that the system has data validation in the fields	
9	System cannot group / index all records for a unique data subject	• Evidence that system can index all data for a unique data subject • Evidence that all records for a unique data subject can be	
10	Data subject access rights cannot be enforced by system	• Evidence that the system can extract data on a record level for provision to data subject	
11	Data subject deletion rights cannot be enforced by system	• Evidence that the system can delete individual records	
12	Data subject correction rights cannot be enforced by system	• Evidence that the system can correct data	
13	System is taken offline maliciously, resulting in service not being delivered to clients.	• Evidence of system monitoring • Evidence of business continuity for system • Evidence of Denial of Service protection	
14	System does not have relevant business continuity provisions in case of catastrophic failure	• Evidence of business continuity plans by department • Evidence of business continuity plans by supplier	
15	Malicious person registers on system to access data	• Evidence of user authentication process	
16	System is compromised and used to deliver malicious software to Trust's infrastructure	• Evidence that the system has been fully tested / accredited to ensure that it cannot be compromised using technical tools • Evidence of monitoring of unusual activity • Evidence of integrity verification on system code	

17	Components of system installed on Trust infrastructure used to compromise the infrastructure	• Evidence that any components that are needed have been fully accredited and checked • Evidence that components do not rely on communication with third parties	
18	System allows malicious software to be transferred from 3rd party network to Trust infrastructure	• Evidence that any communication with third parties is scanned and verified • Evidence of integrity verification of all data transmitted to Council infrastructure	
19	Bandwidth used by system causes availability issues for corporate applications based on the internet	• Details of bandwidth used by system for BAU	
20	Audit logs do not provide enough detail for transactions on data	• Details of logging conducted by system • Assessment of logging capability compared to requirement for category of data being processed	

APPENDIX B: DATA PROTECTION IMPACT ASSESSMENT REGISTER

Date	Reference	Signatories	Department e.g. teaching, IT, HR etc.	System