Data Protection Impact Assessment Policy

Reviewed and adopted by the Board of Trustees: 12th September 2024
Date of next review: Q3 2025

Data Protection Impact Assessment Policy

Introduction

This policy outlines the approach of Construction Youth Trust (the Trust) towards Data Protection Impact Assessments (DPIAs) in compliance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. This policy is designed to ensure that the Trust complies with its legal obligations and is committed to protecting the privacy and personal data of individuals who engage with the Trust.

1. Responsibilities of the controller

1.1 As the controller, the Trust is responsible for ensuring that DPIAs are carried out when required, and that all DPIAs are carried out in compliance with the GDPR and the Data Protection Act 2018. The Trust will appoint a DPIA lead to oversee the DPIA process and ensure that all necessary steps are taken to protect the privacy and personal data of individuals.

2. What is a DPIA?

2.1 A DPIA is a risk assessment process that is designed to identify, assess, and mitigate any potential risks to the privacy and personal data of individuals who engage with the Trust. It is a legal requirement under GDPR for organisations to conduct DPIAs when processing data that is likely to result in a high risk to the rights and freedoms of individuals.

3. When do we need a DPIA?

3.1 The Trust will carry out a DPIA when:

- Introducing new systems, processes, or technologies that involve the processing of personal data.
- Making significant changes to existing systems, processes, or technologies that involve the processing of personal data.
- Conducting large-scale data processing activities, including profiling and automated decision-making.
- Processing special categories of personal data or criminal conviction and offence data.

4. At what point do we begin a DPIA?

4.1 The Trust will begin a DPIA as early as possible in the planning process for any new systems, processes or technologies that involve the processing of personal data. This will allow us to identify any potential risks to the privacy and personal data of individuals and take steps to mitigate those risks before the processing begins.

5. How do we carry out a DPIA?

5.1 The Trust will follow the following steps when conducting a DPIA:

- **Identify the need for a DPIA**

The Trust will identify the need for a DPIA when introducing new systems, processes, or technologies that involve the processing of personal data.

- **Describe the processing**

The Trust will describe the nature, scope, context and purposes of the processing.

- **Consider necessity and proportionality**

The Trust will assess whether the processing is necessary for the intended purposes and whether it is proportionate to the risks to the individual's rights and freedoms.

- **Identify and assess risks**

The Trust will identify and assess the potential risks to the privacy and personal data of individuals who engage with the Trust.

- **Identify measures to mitigate risks**

The Trust will identify and evaluate measures to mitigate the risks to the privacy and personal data of individuals.

- **Review and update the DPIA**

The Trust will review and update the DPIA when there are changes to the processing or the risks associated with it.

6. Links with other policies

6.1 This subject access request policy is linked to the Trust's:

- Data Protection Policy
- Freedom of information Policy
- Security Incident and Data Breach Policy
- Records Retention and Deletion Policy
- Information Sharing Policy
- Information Security Policy

APPENDIX 1
DPIA TEMPLATE

DPIA

New process:		Date:	

These questions are intended to help you decide whether a PIA is necessary. Answering 'yes' to any of these questions is an indication that a PIA would be a useful exercise. You can expand on your answers as the project develops if you need to.

You can adapt these questions to develop a screening method that fits more closely with the types of project you are likely to assess.

You should start to fill out the template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

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

Submitting Controller Details

Name of controller	
Subject/title of DPO	
Name of controller contact /DPO (delete as appropriate)	

STEP 1: Identify the need for a DPIA

Explain broadly what the project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

STEP 2: Describe the process

Describe the 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?

Describe the 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?

Describe the 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)?

Describe the 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: Access 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? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

STEP 5:

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

STEP 6: Identify 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**	**Residual risk**	**Measure approved**
		Eliminated reduced accepted	Low medium high	Yes/no

STEP 7: Sign off and record outcomes

Item	Name/position/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
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
Comments:		
Consultation responses reviewed by:		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