Catch22 Group Policy

Data Protection Impact Assessment Policy

Contents

1. Purpose 2

2. Scope 2

3. What is a Data Protection Impact Assessment? 2

3.1 When is an assessment required? 2

3.2 Assessment Responsibilities 3

4. Transferring Information Outside of the UK 3

5. Assessment Sign Off 4

Policy Compliance 4

Related policies 5

Document Version Control 5

Annex 1: Equality Impact Assessment 5

Catch22 reserves the right to amend this policy, following consultation, where appropriate.

Policy Owner:	Michael Oniyitan
Queries to:	Michael Oniyitan
Date created:	31/05/2018
Date of last review:	13/04/2026
Date of next review:	13/04/2027
Catch22 group, entity, hub:	Catch22 Charity
4Policies level (all staff or managers only)	All Staff

1. Purpose

Catch22 is committed to ensuring that it protects and manages the personal information that it holds while doing business with the highest care and respect. This policy has been created to outline the importance of Data Protection Impact Assessments, how they affect the protection of personal data we process, how we ensure compliance with the UK General Data Protection Regulation, and the responsibilities for the completion of an assessment.

2. Scope

This policy applies to all company employees, volunteers, secondees, contractors, agency workers, and external users. The policy applies to data processing regardless of systems, data formats, and processing activities.

3. What is a Data Protection Impact Assessment?

Under Article 35 of the UK General Data Protection Regulation (UK GDPR), there is a legal requirement for an impact assessment to be undertaken where data processing is likely to result in a high risk to the rights and freedoms of living people.

The aim of a Data Protection Impact Assessment (DPIA) is to understand and assess all how Catch22 want to use information to identify risks to the data subjects and risks to compliance with UK GDPR. A completed DPIA allows the Data Protection Team to identify areas of non-compliance and solutions to be implemented which would lower any risk to data subjects.

A DPIA must be completed using the current Catch22 template as it covers all requirements of the UK GDPR. If a DPIA has been completed using a third party's template, the Data Protection Team can review it and advise once sent to DPO@catch-22.org.uk.

While there is a template to utilise, a DPIA itself is the process that includes completion of the form, analysis of answers, identification of corrective actions, implementation of the corrective actions, and then approval of the DPIA.

3.1 When is an assessment required?

Any processing of information which is likely to result in a high risk to the rights and freedoms of Catch22 stakeholders requires a DPIA to be completed. The UK GDPR outlines specific situations where a DPIA must be completed:

1. We want to use new technology
2. We want to profiling or process special category data to decide whether someone is allowed access to a service

3. We want to profile individuals on a large scale
4. We want to process biometric data
5. We want to process genetic data
6. We want to match or combine data from multiple sources
7. We want to collect personal data from a source that is not the individual without providing them with a privacy notice first
8. We want to track an individual's location or behaviour
9. We want to profile children or target services at them
10. We want to process data that may endanger the individual's physical health or safety in the event of a security breach

Regardless of the reasons listed above, at a minimum, the DPIA template must be used to complete the screening questions which will indicate whether a full DPIA is required.

The template can be gathered from the Catch22 intranet or directly from DPO@catch-22.org.uk.

3.2 Assessment Responsibilities

When taking into account the aim of an assessment, information is to be provided by those that propose data processing (typically a service or corporate service function) through the template. The Data Protection Team then assess the DPIA outlining any areas that require attention prior to processing commencing.

If for any reason, there is not a DPIA in place for existing processing, a DPIA ***MUST*** be completed and corrective actions implemented where risks are identified.

The Data Protection Team are responsible for providing:

1. Guidance as required in completing a DPIA
2. Assessment of the DPIA once first draft is completed
3. Identified risks and recommendations for treating that risk

As the Data Protection Team do not know the entirety of the processing being recommended, the completion of the DPIA itself is the responsibility of the service or function that would like to process data using the proposed approach.

DPIAs will be stored centrally by the Data Protection Team within the Information Security Management System.

It is the responsibility of the service or function to ensure the DPIA is reviewed at least annually or when requested by the Data Protection Team.

4. Transferring Information Outside of the UK

There are additional legal obligations and responsibilities surrounding the transfer of information outside of the United Kingdom. This includes using systems that will process information on systems outside of the UK, regardless of whether the final storage of the data is in the UK.

Where this is known to be the case, a DPIA ***MUST*** be completed and checks against existing privacy notices and service contracts assessed.

All international transfers require the use of transfer mechanisms including International Data Transfer Agreements (IDTA), UK addendums to EU Standard Contractual Clauses (SCCs), and Transfer Risk Assessments (TRAs).

The use of cloud systems where data would be processed outside of the UK (for example a system like Salesforce setup to use servers based in the US), would be an international transfer.

No international processing can occur without approval from the Data Protection Officer and the relevant transfer mechanisms.

5. Assessment Sign Off

The sign off process for a DPIA is dependent on the final risk level identified. Risks are to be identified, impact and likelihood logged, and mitigations documented. The highest severity risk sets the final risk level for the DPIA, final sign off is as below:

1. **Risk Level Low** – Project can proceed
2. **Risk Level Medium** – Recommended Actions to be implemented
3. **Risk Level Medium/High** – Recommended Actions to be implemented
4. **Risk Level High** – Actions for implementation recommended and Senior Information Risk Owner approval required
5. **Risk Level Catastrophic** – Not to proceed until full sign off by Chief Officers

Policy Compliance

Compliance Measurement

The Information Security Management Review Team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

Exceptions

Any exception to the policy must be approved and recorded by the Information Security Manager in advance and reported to the Management Review Team.

Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Continual Improvement

The policy is updated and reviewed as part of the continual improvement and process.

Related policies

- Data Protection Policy Suite
- Information Security Policy Suite

Document Version Control

	Last Modified	Last Modified By	Changes Made
1.0	31/01/2023	Beverley Clark	Policy Live
2.0	30/06/2023	Beverley Clark	Annual Review Completed
3.0	13/04/2026	Ben Wright	Full rebuild of policy

Annex 1: Equality Impact Assessment

Summary

This EIA is for:	Data Protection Impact Assessment Policy
EIA completed by:	Michael Oniyitan – Data Protection Officer
Date of assessment:	24/02/2026
Assessment approved by:	Assistant Director - Justice

Catch22 is committed to always: avoiding the potential for unlawful discrimination, harassment and victimisation; advancing equality of opportunity between people who share a protected characteristic and those who do not; and,

foster good relations between people who share a protected characteristic and those who do not.

An Equality Impact Assessment (EIA) is a tool for identifying whether or not strategies, projects, services, guidance, practices or policies have an adverse or positive impact on a particular group of people or equality group. Whilst currently only public bodies are legally required to complete EIA's under the Equality Act 2010, Catch22 has adopted the process in line with its commitment to continually improve our equality performance.

Policy owners are required to complete or review the assessment indicating whether the policy has a positive, neutral or negative impact for people who it applies to and who share one or more of the 9 protected characteristics under the Equality Act 2010.
Definitions are based on the Equality & Human Rights (EHRC) guidance.

Objectives and intended outcomes
This Equality Impact Assessment has been completed to ensure that the Data Protection Impact Assessment (DPIA) Policy supports the fair, lawful, and proportionate processing of personal data and does not create barriers or disadvantage for individuals who share a protected characteristic. The policy establishes a structured and risk-based approach to identifying, assessing, and mitigating risks to the rights and freedoms of individuals where high-risk processing is proposed. Its intended outcome is to ensure that privacy risks are identified early, mitigated appropriately, and that decision-making around data processing is transparent, accountable, and compliant with UK data protection legislation.

Potential Impacts, positive and negative

Equality Area	Positive	Neutral	Negative	Please give details including any mitigation for negative impacts
Age Does this policy impact on any particular age groups or people of a certain age?	☒	☐	☐	
Disability Does this policy impact on people who have a physical or mental impairment which has a substantial and long-term adverse effect on that person's ability to carry out normal day to day activities?	☒	☐	☐	
Gender reassignment (transsexual, transgender, trans) Does this policy impact on people who are transitioning from one gender to another (at any stage)	☒	☐	☐	
Marriage and civil partnership Does this policy impact on people who are legally married or in a civil partnership?	☐	☒	☐	
Pregnancy and maternity (in work this is linked to maternity leave, non-work this is for 26 weeks after giving birth) Does this policy impact on people who are pregnant or in their maternity period following the birth of their child?	☒	☐	☐	
Race	☒	☐	☐	

Does this policy impact on people as defined by their race, colour and nationality (including citizenship) ethnic or national origins				
Religion and belief Does this policy impact on people who practice a particular religion or none, or who hold particular religious or philosophical belief or none?	☒	☐	☐	
Sex Does this policy impact on people because they are male or female?	☐	☒	☐	
Sexual orientation Does this policy impact on people who are sexually attracted towards their own sex, the opposite sex or to both sexes?	☒	☐	☐	

More information/notes

Please add any links to key documents or websites to evidence or give further detail on any impacts identified.
• The DPIA Policy is procedural and governance-focused and applies equally across all Catch22 services and functions. • The policy does not introduce new processing activities; it governs how proposed processing is assessed and approved. • Oversight by the Data Protection Team and escalation routes to the SIRO or Chief Officers ensure consistent and proportionate decision-making. • No negative equality impacts have been identified. The policy is considered to have an overall positive impact by embedding fairness, accountability, and protection of individual rights at the earliest stage of data processing design.

Data Protection Impact Assessment Policy
Version 3.0