Catch22 group policy

Data Protection – Data Privacy Impact Assessment policy

Contents

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

Policy Owner:	*Data Protection Officer*
Queries to:	*Data Protection Officer*
Date created:	*31 May 2018*

Date of last review:	*November 2024*
Date of next review:	*November 2025*
Catch22 group, entity, hub:	*Catch22 group*
4Policies level (all staff or managers only)	*All staff*

Version	Last modified	By	Changes Made
1.0	31/01/2023	Beverley Clark	Policy review – Title amended
2.0	30/06/2023	Beverley Clark	Policy review – no changes made.
2.1	01/07/2024	Jamie Wright	Extension to end date
2.2	10/09/2024	Jamie Wright	Extension to end date
2.3	19/11/2024	Michael Oniyitan	Updated DPIA template

Catch22 UKGDPR standards

When processing personal data staff will uphold the following standards, where possible:

- **Model of least privilege**

  Staff will ensure that security controls are implemented, to data held physically and electronically, to ensure that personal data is only accessed by staff that have a defined need to access it.

- **Data minimisation**

  Staff will limit the collection of personal information to that which is directly relevant and necessary to accomplish a specified purpose.

- **Data subject rights**

  Staff will ensure that the rights that are afforded to individuals under the UKGDPR are upheld appropriately and in accordance with the regulation and associated legislation.

- **Accountability**

  Staff will adhere to and remain compliant with the seven UKGDPR principles and contribute to demonstrating the organisations compliance.

- **Anonymisation, Pseudonymisation and Encryption**

  Where possible and appropriate staff will look to anonymise/pseudonymise and encrypt personal data to protect the privacy rights of individuals.

1. Policy statement

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. Conducting data protection impact assessments (DPIA) will be an essential element that will contribute to achieving this commitment. Conducting DPIA's ensures that the privacy rights of Catch22's stakeholders (service users, staff, volunteers, contractors, supporters) are taken into consideration and any risks to those rights are suitably mitigated prior to embarking on a new way of processing personal data. This ensures that privacy is placed at the forefront of any project and new processing activity. Article 35 of the United Kingdom General Data Protection Regulation (UKGDPR) legally requires an impact assessment to be undertaken where a type of processing, using new technologies, is likely to result in a high risk to the rights and freedoms of natural (living) persons.

2. Scope

The aim of this policy is to ensure that staff are aware of their responsibilities with regard to conducting DPIA's for new processing systems, activities and projects. The policy aims to provide clear detail as to how and when to conduct a DPIA.

3. What is a DPIA?

DPIA's are designed to allow organisations to assess the risks to the privacy of the individuals that a proposed processing activity may affect to ensure that their privacy, dignity, and well-being are not adversely impacted. Performing a DPIA at the early stage of a project puts the privacy of the individuals at the forefront and avoids any issues being discovered at a later stage. The assessment allows solutions to issues to be considered and mitigated against prior to initiating the project, which allows for more robust and confident processing of personal/special category data.

4. When is a DPIA required?

A DPIA must be undertaken before beginning any type of processing which is likely to result in a high risk to the rights of Catch22's stakeholders. To assess the level of risk, a DPIA must consider both the likelihood and the severity of any impact on individuals. It should look at risk based on the specific nature, scope, context, and purposes of the processing.

UK Data Protection Legislation requires DPIA's to be undertaken when the following are proposed:

- using new technologies
- using profiling or special category data to decide on access to services
- profiling individuals on a large scale
- processing biometric data
- processing genetic data
- matching or combine datasets from different sources
- collecting personal data from a source other than the individual without providing them with a privacy notice
- tracking individual's location or behaviour

- profiling children or target services at them; or
- processing data that might endanger the individual's physical health or safety in the event of a security breach.

Data protection law also requires that DPIA's are undertaken where the following is proposed:

- using systematic and extensive profiling with significant effects.
- processing special category or criminal offence data on large scale; or
- systematically monitoring publicly accessible places on a large scale.

In cases where there is no indication of a high risk to the individual, it remains good practice to conduct a DPIA for any major new project involving the use of personal data.

5. Objectives of the DPIA

The key outcomes that a DPIA should achieve are:

- the identification of the project's potential privacy impacts and risks.
- appreciation of those impacts from the perspectives of all stakeholders.
- an understanding of the acceptability of the project and its features by the organisation and people that will be affected by it.
- management of information risk, and other risks to privacy, by:
    - *identification and assessment of less privacy invasive alternatives.*
    - *identification of ways in which negative impacts on privacy.*
    - *where negative impacts on privacy are unavoidable, clarity as to the business need that justifies them; and*
- documentation of the outcomes.

6. Transferring information outside of the UK

There are a number of additional requirements and legal obligations surrounding the transfer of information outside the UK. If this is identified as an aspect of of the DPIA you must seek guidance from the DPO immediately.

7. Managing a DPIA

The responsibility for conducting a DPIA is placed upon the project lead. Depending upon the nature and type of the project the task of conducting the DPIA may be delegated. However, any person delegated to undertake a DPIA must have a detailed understanding of the project, the processing activities that are proposed and must be in a position to influence the design and development of the project.

The Data Protection Officer (DPO) will provide advice and assistance to the project lead as required. The DPO will also be responsible for maintaining a DPIA log and will retain all copies of the pre-DPIA questionnaires and impact assessments. Once a DPIA has been submitted to the DPO it will be circulated to all subject Matter experts for their review, guidance and/or approval. The DPO will then formally respond and will send to the appropriate person for signature.

The following delegations of authority apply:

- High residual risk – requires the sign off of the responsible Chief Officer.
- Medium residual risk – requires the sign off of the responsible Director.
- Low residual risk – requires the sign off of the service manager.

8. Definitions

Personal data means data which relate to a living individual who can be identified –
(a) from those data, or
(b) from those data and other information, which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Sensitive/Special Category personal data means personal data consisting of information as to-
(a) the racial or ethnic origin of the data subject,
(b) their political opinions,
(c) their religious beliefs or other beliefs of a similar nature,

(d) whether they are a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
(e) their physical or mental health or condition,
(f) their sexual life,
(g) the commission or alleged commission by them of any offence, or
(h) any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

The presumption is that, because information about these matters could be used in a discriminatory way, and is likely to be of a private nature, it needs to be treated with greater care than other personal data. In particular, if we are processing sensitive personal data, we must satisfy one or more of the conditions for processing which apply specifically to such data, as well as one of the general conditions which apply in every case.

Processing, in relation to information or data, means obtaining, recording, or holding the information or data or carrying out any operation or set of operations on the information or data, including –
(a) organisation, adaptation or alteration of the information or data,
(b) retrieval, consultation or use of the information or data,
(c) disclosure of the information or data by transmission, dissemination or otherwise making available, or
(d) alignment, combination, blocking, erasure or destruction of the information or data.
The definition of processing is very wide, and it is difficult to think of anything an organisation might do with data that will not be processing.

Data subject means an individual who is the subject of personal data.
In other words, the data subject is the individual whom particular personal data is about. The Act does not count as a data subject an individual who has died or who cannot be identified or distinguished from others.

Data protection impact assessment, a data protection impact assessment (DPIA) is a process to help you identify and minimise the data protection risks of a project.
A DPIA must be undertaken for certain listed types of processing, or any other processing that is likely to result in a high risk to individuals' interests. You can use our screening checklist to help you decide when to do a DPIA.
For all other definitions please see the Data Protection: Over-arching Policy 2021.

9. Related policies

Data Protection Policy Suite

Catch22 Data Protection Document

Data Protection Impact Assessment

Data Protection Impact Assessment Information

Data Processing Activity/System Title	
DPIA Author	
DPIA Owner	
Service Name	
Date of DPIA	

Please indicate anything below that applies to this DPIA

New Service	
New Project	
New System	
New Data Processing Activity	
Existing System or Processing Activity	
Sharing Personal Information with a Third Party	
Other (please clarify)	

To be completed by the Data Protection Officer once DPIA has been accepted

DPIA Review Date	
DPIA Reference Number	

Section 1 – Screening Questions

Please complete the screening questions below, these are here to help identify whether a full DPIA is required. **If you answer yes to one or more of the questions below, a full DPIA *MUST* be completed.**

If you answer no to each of the questions below, please mark the *"Is a full DPIA required?"* question as no, sign in the relevant section, and send back to DPO@catch-22.org.uk.

#	Question	Yes	No
1	Will personal information be used for evaluation or scoring?		
2	Will personal information be used for automated decision-making that could have a significant impact on the individual?		
3	Will personal information be processed through systematic monitoring of individuals?		
4	Will there be processing of sensitive data?		
5	Will there be large scale processing of data?		
6	Will there be processing of data concerning vulnerable data subjects?		
7	Will processing of information include the use of innovative technology?		
8	Will processing of this information prevent data subjects from exercising a right or using a service or contract?		
9	Will there be processing of biometric or genetic data?		
10	Will processing include combining, comparing, or matching data from multiple sources?		
11	Will Catch22 be processing personal data without providing a privacy notice directly to the individual?		
12	Will there be processing of personal data that tracks individuals' online or offline location or behaviour?		
13	Will there be processing of children's personal data?		
14	Will there be processing of personal data that could result in a risk of physical harm in the event of a security breach?		
15	Is there a change to the nature, scope, context, or purposes to existing processing?		

	Yes	No
Is a full DPIA required?		

Completed By:
Completion Date:
Signed By:
Signature:

If a full DPIA is ***NOT*** required, please send this form to DPO@catch-22.org.uk

If a full DPIA ***IS*** required, please complete questions 16 to 29 below.

Section 2 – Data Processing Activity

It is important for us to understand the type of data to be processed and the processing activity/system itself. This is to enable us to ensure we can identify any changes required to maintain compliance with UK Data Protection Legislation.

What data is being processed?

Data Type	Enter X Where Applicable

Name, Address, DOB, Phone, Email	
Financial Information	
Religious Beliefs	
Medical/Health Information	
Criminal Offenses/Convictions	
Audio or Visual Recordings	
Location Data	
Biometric or Genetic Data	
Ethnicity	
Other – Please State Below:	

Who is the data about that is being processed?

Data Subject Type	Enter X Where Applicable
Employees, Former Employees, or Volunteers	
Customers, Former Customers, or Prospective Customers	
Suppliers, Former Suppliers, or Prospective Suppliers	
Members of the Public	

Describe the people whose data is being processed including a description of their relationships with Catch22.

Would data subjects expect their personal data to be used in the ways envisaged? Include a justification if it is within their reasonable expectations.

Processing System or Activity Overview

What is the purpose of the processing activity and what Catch22 service does it support?

What are the expected benefits for Catch22 and individuals from the processing?

How is the data sourced or collected, and where is it stored and used?

Who is expected to have access to the data and who is it to be shared with?

How often is data expected to be processed, for how long, and what geographical area is covered?

Is Catch22 the Data Controller, the Data Processor, or a Joint-Controller?

The Data Controller is:	Enter X Where Applicable
Catch22 Only	
Catch22 and a Joint Controller	[Insert other organisation(s) names]
Catch22 and a separate Controller	[Insert other organisation(s) names]
Other Organisations Only	[Insert other organisation(s) names]
Not Yet Known	[Insert why this is not yet known]

If you're not sure, the DPO can assist once the rest of the DPIA has been completed.

Who will receive the data, what is their role in this processing activity, and what is their relationship to each other?

Recipient	Data they will receive	Relationship to other Recipients

For each of the recipients listed above, is there a contract or information sharing agreement?

Where any of the recipients above are Joint Controllers with Catch22, who will be responsible for managing risks?

Describe the infrastructure and assets on which the data processing activity will be completed

Approximately, how many individuals are affected by this activity?

Section 3 – Data Protection Principles

What is the lawful basis for this processing to be completed?

If unsure, please use the ICO tool here: Lawful basis interactive guidance tool | ICO

If still unsure, the DPO can assist with this once the rest of the DPIA has been completed.

Lawful Basis	Enter X Where Applicable
We are processing personal data with data subject consent	
We are processing personal data for the performance of a contract	
Personal data is processed to comply with a legal obligation to which Catch22 is subject	
Personal data is processed to protect the vital interests of the data subject	
Personal data is processed for the performance of a task carried out in the public interest or in the exercise of official authority vested in Catch22	
Personal data is processed for the purposes of Catch22's or a third party's legitimate interests	
We are processing criminal offence data under control of an official authority	
We are processing criminal offence data with a DPA 2018 Schedule 1 condition as listed below:	

What is the lawful basis for processing of Special Category Data?

*Where special category data (*Special category data | ICO) is to be processed, there are stricter requirements for when that data can be processed.

We must identify a lawful basis for processing this data, please choose the relevant basis below.

If unsure, the DPO can assist once the rest of the DPIA has been completed.

Lawful Basis	Enter X Where Applicable
Explicit Consent	
Employment, Social Security, and Social Protection	
Vital Interests	
Not-for-profit bodies	
Made public by the data subject	
Legal claims or judicial acts	
Substantial Public Interest *	
Health or Social Care	
Public Health	
Archiving, Research, and Statistics	

**Where substantial public interest is to be used, we must cite the specific conditions from Data Protection Act 2018 and have a policy in relation to the condition.*

Where substantial public interest is the lawful basis, our conditions are:

How are you going to ensure only the data necessary is to be processed?

How are you going to ensure the data being processed is kept accurate?

How are you going to ensure the data is kept secure? Please include any security certification held where appropriate.

Is a data retention schedule in place and how long is the data to be processed for?

Data Subjects Rights

If consent is to be used as a lawful basis for processing, is there is a withdrawal of consent process in place and if so, what is it?

Data Subjects have the right to be informed – typically this would be through a privacy notice supplied to them when first interacting with Catch22. Is a privacy notice in place and to be supplied?

What is the process for managing a Subject Access Request for this activity/data?

Is data to be transferred outside of the UK? If so, has this been checked with Cyber Security or Data Protection?

Is data to be transferred outside of the EU? If so, has this been checked with Cyber Security or Data Protection?

Has there been a consultation completed for this processing? If so, who was involved and what were the outcomes?

Section 4 – Risk Assessment

It is vital that we identify any risks that are posed to individuals as a result of the processing outlined in this DPIA.

When identifying a risk, please identify the Impact of that risk on an individual or Catch22 if it were to occur and the likelihood of the risk occurring. These can be rated from 1 to 5 using the table below:

Impact	Description
1. Negligible	Negligible reputational or financial impact – 1% or less of current reserves
2. Minor	Slight reputational damage or financial impact – 5% or less of current reserves
3. Moderate	Some reputational damage or financial impact where changes are required to maintain quality
4. Significant	Significant reduction in service/quality, significant reputational damage including some national coverage, or heavy financial impact
5. Critical	Irrecoverable reputational damage, organisation or individual may not recover from financial impact, or service is down for more than 3 days

Likelihood	Description
1. Very Unlikely	Highly unlikely to occur – less than once in the next 10 years
2. Unlikely	Likely to happen once within the next 5 years
3. Possible	Likely to happen once in the next 2 years
4. Likely	Likely to happen within the next 6 months
5. Very Likely	Likely to happen within the next month

Risk Description	Impact	Likelihood	Mitigations or Actions

Section 5 – DPO Review

DPO Recommended Actions

DPO Recommended Action	Date Implemented

Final Risk Level

Please take the highest risk identified in the risk assessment section as the final risk level and utilise the guidance in the table below.

Risk level	Mark where applicable
Low (1 to 8) – Project can proceed	
Medium (9 to 12) – Recommend Minor Actions to be implemented	
Medium/High (13 to 15) – Recommend Actions to be implemented	
High (16 to 24) – Recommend Actions and send to SIRO for signoff	
Catastrophic (25) – Not to proceed until signed off by Chief Officers	

Sign Off

To be completed by the Data Protection Officer	
Comments	
Signature	
Signed By:	
Date of Sign Off:	

Annex 1: Equality Impact Assessment

1. Summary

This EIA is for:	Data protection: privacy impact assessment policy – January 2021
EIA completed by:	Beverley Clark, Data Governance Manager
Date of assessment:	27th May 2021
Assessment approved by:	

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 EIA has been completed in order to ensure that the implications and potential impact, positive and negative, of this policy have been fully considered and addressed, whether or not people share a protected characteristic.

2. 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?	☐	☒	☐	

3. More information/notes

Please add any links to key documents or websites to evidence or give further detail on any impacts identified.