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:	*Governance & Risk*
Queries to:	*Data Governance Manager*
Date created:	*31 May 2018*

Date of last review:	*June 2023*
Date of next review:	*June 2024*
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.

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 in order 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 in the course of doing business with the highest care and respect. Conducting data protection impact assessments (DPIA) will be an important 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, in particular 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 Privacy Impact Assessment Form

DATA PROTECTION IMPACT ASSESSMENT	

This Data Privacy Impact Assessment form should be completed as part of the business case for all new information systems, projects, processes or services which involve the use of personal sensitive data or business sensitive data or a change that will significantly amend the way in which personal sensitive data or business sensitive data is handled.

OVERVIEW			
1	The name of the new process, system, project or service?		
2	What is the new process, system or service purpose or main aims?		
SUPPLIER OVERVIEW			
3	Has the supplier of the system implemented ISO27001? If so please provide a copy of the ISO27001 certification		
3a	Does the supplier of the system hold Cyber Essentials Plus?:		
DATA PROCESSING			
4	Who is the information processed about? (Also known as data subjects)		**Employees**
			Service users
			Volunteers
			Students
			Third parties e.g. families, gang members
			Partner businesses or organisations
			Other:
5	What are the Data Classes that will be held on the system?		**Personal sensitive details** (name, address, Postcode, Date of Birth, NI number, NHS number)
			Family, lifestyle and social circumstances (marital status, housing, travel, leisure activities, membership of charities)
			Education and training details (qualifications or certifications, training records etc)

			Employment details (career history, recruitment and termination details, attendance details, appraisals etc)
			Financial details (income, salary, assets, investments, payments etc)
			Criminal proceedings, outcomes and sentences
			Goods or services (contracts, licenses, agreements etc)
			Racial or ethnic origin
			Religious or other beliefs of a similar nature
			Political opinions
			Physical or mental health conditions
			Offences including alleged offences
			Sexual health
			Trade union membership
6	Will this system include data which was not previously collected? If yes have you amended existing privacy notices?		
7	Are you transferring any personal or sensitive data to a country outside the UK? (If so, where)		
TECHNOLOGY			
8	Is the use of Cloud technology being used or considered? If yes, provide the data centre location:		
9	Does the system include new technology that might be perceived as intrusive? (the use of biometrics or facial recognition etc)		
LAWFUL BASIS FOR PROCESSING			
10	What is the legal basis for holding and processing the data?		**Consent**
			Contract
			Legal obligation
			Vital interests

			Public task
			Legitimate interests
11	Do you require the data subjects consent to process or hold the data?		
12	Can the data subjects opt-out of their data being processed?		
13	How will you tell the data subjects about the use of their data?		
14	Have you assessed the likelihood of the loss or damage of the data causing distress, harm or damage to data subjects concerned?		
ACCESS			
15	Who will use the system and have access to the data?		
16	How often will the system be audited?		
DATA STORAGE			
17	Where will the data be stored?		
18	Which format will the data be stored in?		**Electronic**
			Paper
			Verbal
			Other:
DATA SHARING			
19	How will the data be shared?		
20	Are there any Information Sharing Agreements or protocols in place?		
DATA SECURITY			
21	What security measures have been undertaken to protect the data?		

	What access controls will be in place e.g. user credentials (log-in and password), smartcard? Who will have access?	
22	What business continuity plans are in place in case of data loss or damage? (As a result of human error, virus, network failure, theft, fire, floods etc.)	
ON-GOING USE OF DATA		
23	Will the project interfere with the privacy under article 8 of the Human Rights Act?	
24	Will the data be used to send direct marketing messages?	
25	What is the data retention period for this data? (The retention schedules are set out in the Catch22 Records Management Policy)	

Risk Assessment – Data Subject's *Rights and Freedoms*:

Using the table below, assess if there is a risk that the processing/information sharing may give rise to *discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of control/confidentiality*?

IMPACT	5 Catastrophic	**5**	**10**	**15**	**20**	**25**
	4 Major	**4**	**8**	**12**	**16**	**20**
	3 Moderate	**3**	**6**	**9**	**12**	**15**
	2 Low	**2**	**4**	**6**	**8**	**10**
	1 Negligible	**1**	**2**	**3**	**4**	**5**
		1 Rare	2 Unlikely	3 Possible	4 Likely	5 Almost Certain
		LIKELIHOOD				

SCORE: **Impact =** **Likelihood =** **TOTAL =** **Provide a summary of identified risks, and mitigation plan:**

Information Asset Owner:

Who is the Information Asset Owner: Name / role: Department / team: Contact details:

On completion – submit the completed form to both: dpo@catch-22.org.uk and cyber.security@catch-22.org.uk

THIS SECTION TO BE COMPLETED BY CYBER SECURITY MANAGER	
ISO27001/Cyber Essential Plus certification received?	
Comments	
Date of sign off:	

THIS SECTION TO BE COMPLETED BY DATA PROTECTION OFFICER	
ICO Registration number & details received?	
IG Toolkit compliance seen? (Health & Social Care)	
ODS Code provided? (Health & Social Care)	
Comments	
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.