Catch22 Group Policy

Data Protection Overarching Policy

Contents

1. Purpose 2
2. Scope 2
3. Legal Requirements 2
4. Statement of Principles 2
5. Responsibilities 3
6. Data Processing Locations 3
7. Risk Management 4
8. Breach of Policy 5
9. Training and Awareness 5
10. Policy Compliance 6
11. Related policies 6
12. Document Version Control 7

Annex 1: Equality Impact Assessment 8

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

The purpose of this policy to ensure all staff are aware of their responsibilities and obligations in relation to Data Protection and inform members of the public on how Catch22 complies with all UK Data Protection. This policy sets out the governance framework for privacy management across the organisation.

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. Legal Requirements

Catch22 must adhere to emerging and amended Data Protection Legislation where applicable including:

- Data Protection Act 2018
- UK General Data Protection Regulation
- Privacy & Electronic Communications Regulation 2003
- Human Rights Act 1998 (Article 8)
- Data (Use and Access) Act 2025

4. Statement of Principles

Catch22 will ensure that data subjects are provided with a clear and unambiguous notice detailing:

- What information we hold
- Why we hold it
- Who it is shared with and why
- How long it will be held for
- Who the data controller is and how to contact them
- How to exercise their rights
- The legal basis for processing their data

Catch22 will respond to data subject rights requests in a timely way in accordance with Data Protection Legislation providing clear information for why a subject rights request cannot be completed where applicable. These rights include:

- Right to be Informed

- Right of Access (Subject Access Request)
- Right to Rectification
- Right to Erasure
- Right to Restrict Processing
- Right to Data Portability
- Right to Object

Catch22 will implement appropriate organisational and technological security measures to protect the data we hold based on the level of assessed risk and in compliance with our Information Security policies.

Catch22 will only collect the data that is needed for the specified purpose and ensure that the data is accurate, necessary, updated where required and relevant to the purpose for which it is collected. In addition, Catch22 will ensure that information is only accessible to those that require access and information will only be kept for as long as is necessary to fulfil the purpose of processing.

All new services or methods of delivery will be suitably assessed for privacy and information risks using Data Protection Impact Assessments where necessary. This analysis will allow the implementation of privacy by design into the relevant processes.

Catch22 have a Data Protection Officer role in place who ensures that the organisation is kept aware of its responsibilities under UK Data Protection Legislation, maintains and updates the ICO registration, and provides guidance to all stakeholders regarding Data Protection compliance matters.

5. Responsibilities

Data Protection is the responsibility of each and every member of staff in Catch22. Whilst the Data Protection Officer is in place to provide the relevant guidance for Catch22 staff, is the responsibility of every staff member to ensure that information is held appropriately, securely, and treated with respect.
The Senior Information Risk Owner (SIRO) provides executive oversight of information risk and ensures that data protection and information risks are appropriately managed and resourced across Catch22. The SIRO works closely with the Data Protection Officer and Information Security Manager to ensure compliance with Data Protection Legislation and effective risk management.

Individual members of staff are responsible for ensuring they act within the scope of the law, and seek further advice from DPO@catch-22.org.uk where necessary.

6. Data Processing Locations

There are legal obligations that must be met before information can be transferred out of the European Economic Area (EEA). Catch22 primarily processes personal data within the United Kingdom. Some services, systems, or suppliers may involve processing within the EEA or internationally. Where this occurs, appropriate legal, contractual, and risk-based safeguards will be implemented prior to processing. Where this is needed, guidance must be sought from DPO@catch-22.org.uk **before** any processing is completed outside of the UK.

In some cases, this is to ensure that the relevant legal mechanisms are in place to allow lawful transfer and processing of information including the build and implementation of tools such as International Data Transfer Agreements (IDTA), Transfer Risk Assessments (TRA), and inclusion of Standard Contractual Clauses (SCCs) where required. In other cases, while the legal mechanisms are in place, contractual requirements may dictate specific locations for the processing of information. It is therefore vital that both contractual and legal requirements are met before processing of this nature goes ahead.

No international transfers may occur without contractual assurances and documented approval through DPO@catch-22.org.uk.

7. Risk Management

Risks to Data Protection Legislation compliance must be identified where possible, treatments documented, and ongoing review completed. Risks related to Data Protection will be identified through Data Protection Impact Assessments, review of internal and external issues, changes to UK Data Protection Legislation, and incident root cause analysis.

All risks identified are logged on the Data Protection Risk Register and are communicated to senior management on a quarterly basis. Where risks are identified as wider organisational risks, they are raised on the organisational risk register which is then communicated to Catch22's senior leadership and trustees. All risks are rated with either the impact on the organisation or data subject in mind and the likelihood of that risk occurring.

Where processing of data is for the legitimate interests of Catch22, a Legitimate Interest Assessment (LIA) must be completed, this is to be completed with DPO@catch-22.org.uk. An LIA must be completed to assess the risk to data subjects of processing completed in the legitimate interests of Catch22.
All data processing that poses a high risk to the data subject(s) must have a Data Protection Impact Assessment (DPIA) completed. A DPIA is conducted to fully understand data processing to identify any risks to all stakeholders involved including both Catch22 and our service users.

If any staff member identifies a risk regarding potential Data Protection non-compliance, they should contact DPO@catch-22.org.uk immediately..

8. Breach of Policy

The Information Commissioner's Office (ICO) defines a data breach as:

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Data Protection breaches may result in civil enforcement, legal proceedings, and/or regulatory penalties against Catch22. Wilful or reckless breach of this policy and/or UK Data Protection Legislation will be subject to Catch22's disciplinary procedures.

All data breaches must be reported via Datix immediately. Catch22 have a legal responsibility to report breaches to the Information Commissioner's Office (ICO) within 72 hours of a breach occurring if it presents a risk to a data subject's rights and freedoms.

Where a data breach is believed to of occurred, evidence must be preserved including the initial data breach and evidence of correction.

The Data Protection Officer will review all reported data breaches and where appropriate, recommend notifying data subjects of the breach.

9. Training and Awareness

All staff must complete their mandatory annual Information Security and Data Protection training. Where staff have not completed the training, escalation of non-completion will be shared with management with ongoing non completion being escalated further. This may result in disciplinary action.

The training is to be completed through the online training solution which can be found via Catch Connect or through a ticket to cyber.security@catch-22.org.uk.

10. Policy Compliance

Compliance Measurement

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

11. Related policies

- Data Protection Policy Suite
- Information Security Policy Suite
- IS 04 Information Security Risk Management Policy
- IS 05 Information Classification and Handling Policy
- IS 06 Information Security Awareness and Training Policy
- IS 07 Acceptable Use Policy
- IS 17 Information Transfer Policy
- IS 20 Record & Document Management Policy
- IS 22 Incident Response Policy

12. Document Version Control

	Last Modified	Last Modified By	Changes Made
1.0	30/06/2022	Beverley Clark	Policy updated – Data Protection Compliance
2.0	30/06/2023	Beverley Clark	Policy Review – No Changes
2.1	01/07/2024	Jamie Wright	Extension to review date
2.2	10/09/2024	Jamie Wright	Extension to review date
2.3	19/11/2024	Michael Oniyitan	Policy Review – No Changes Made
3.0	13/04/2026	Ben Wright	Policy Review – Rebuilt, structure changed, risk management added, policy changed to DP 01

Annex 1: Equality Impact Assessment

Summary

This EIA is for:	DP 01 Data Protection Overarching Policy
EIA completed by:	Michael Oniyitan
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 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.

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?	☒**Error! Bookmark not defined.**	☐	☐	
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 Data Protection Overarching Policy applies equally to all staff, volunteers, service users, and other individuals whose personal data is processed by Catch22. • The policy does not introduce new processing activities but provides a governance framework that applies consistently across all services. • Oversight by the Data Protection Officer and escalation routes to the SIRO ensure proportionate and consistent decision-making. • No negative equality impacts have been identified. The policy is considered to have an overall positive impact in promoting fairness, accountability, and protection of individual rights.

Data Protection Overarching Policy
Version 3.0