Catch22 Group Policy

Data Processing Policy

Contents

1. Purpose 2

2. Scope 2

3. Key Definitions 2

4. Identifying Processing Requirements 3

5. Processing as a Data Controller 4

6. Processing as a Data Processor 5

7. Use of Sub-Processors 6

8. Internal Processing Rules & Responsibilities 7

9. Use of Third Party Systems & Services 8

10. Policy Compliance 9

11. Related policies 10

12. Document Version Control 10

13. Annex 1: Equality Impact Assessment 11

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

Policy Owner:	Michael Oniyitan, Data Protection Officer
Queries to:	Michael Oniyitan, Data Protection Officer
Date created:	13/04/2026
Date of last review:	-
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's services require personal data to be processed when delivery is underway. This processing is governed by legal requirements within UK Data Protection Legislation along with contractual requirements. This policy governs how processing is identified, authorised, documented, and carried out. It focuses on different processing roles, internal responsibilities, and operational process requirements.

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. Key Definitions

There are terms used throughout this policy that are given meaning by UK Data Protection Legislation, the Information Commissioner's Office, or are standard industry terms that need to be understood. The definition of these terms has been included below for ease of access and understanding.

Processing	This means any operation performed on personal data or sets of personal data. This includes collection, recording, organisation, structuring, storage, alteration, retrieval, consultation, use, disclosure, dissemination, restriction, erasure or destruction.
Controller	A person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Only controllers need to pay the data protection fee.
Joint Controller	Where two or more controllers jointly determine the purposes and means of processing, they are joint controllers.
Processor	A person, public authority, agency or other body which processes personal data on behalf of the controller.
Sub-Processor	A sub-processor is processes personal data on behalf of a processor under contract. This can only be done under the instruction of the controller.
Processing Instructions	All processors must limit data processing to the instructions of the data controller. These instructions are typically documented within a Data Processing Agreement or Data Processing Schedule within a contract.
Personal Data Flow	The movement, processing, or transfer of information relating to a living individual.
Personal Data	Any information relating to a person (a "data subject") who can be identified, directly or indirectly, in particular by

	reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person.
Special Category Data	Sensitive personal data requiring higher protection due to increased risks to individuals. It includes data related to race, political opinions, trade union membership, religion, genetics, biometrics, health, sex life, and sexual orientation.
Criminal Offence Data	Personal data relating to criminal convictions and offences or related security measures. Processing of this data carries specific legal requirements under the UK General Data Protection Regulation.
Shadow IT	The use of software, hardware, or cloud services within an organisation without the explicit approval, knowledge, or oversight of the IT department.
Record of Processing Activity (ROPA)	An inventory of Catch22's processing activities including purpose, data types, recipients, transfer mechanisms, retention times and more. This is a requirement of the UK General Data Protection Regulation.
Data Protection Impact Assessment (DPIA)	A risk assessment process that must be completed as required under the UK General Data Protection prior to any "high-risk" processing activities. The completion of a DPIA helps Catch22 identify and minimise data protection risks posed by proposed processing of personal data.

4. Identifying Processing Requirements

There are several ways to identify new or updated data processing activities. Whenever a new activity is initiated, or an existing one changes, it is essential to notify DPO@catch-22.org.uk so that proper guidance can be given. Processing activities may be recognised by, but are not limited to, the following routes:

- Request for new systems or software
- The implementation of new data collection methods
- The implementation of new suppliers
- New or changing commissioner requirements
- The mobilisation of new services
- Requests for new analysis of existing data
- Requests to share information with a new third party
- Increases in information shared with third parties

Where new or amendments activitiess take placethere are a number of key steps that **must** be taken by staff to ensure we comply with UK Data Protection Legislation. Following these steps not only ensures compliance with UK Law but also protects our service users, Catch22, our staff, and our commissioners from unwanted risk or exposure. The actions required are:

- The completion of a Data Protection Impact Assessment

- Request for guidance from the Data Protection Team (DPO@catch-22.org.uk)
- Discussions with the data controller where we are a data processor and have not been instructed to conduct the new data processing activities
- Updating of the relevant record entry on the Record of Processing Activities (ROPA)
- The updating of relevant privacy notices and, where applicable, consent forms
- Creation and distribution of fair processing notices where applicable
- The build and sign off of Legitimate Interest Assessments where applicable

The Data Protection Team can provide guidance on any of the points above, where assistance is required, an email must be sent to DPO@catch-22.org.uk.

5. Processing as a Data Controller

When Catch22 acts as a Data Controller for data processing, it must closely follow the strict rules set by UK Data Protection Legislation. Data Controllers bear the greatest responsibility for meeting these requirements, which includes following Data Protection principles and ensuring that Data Processors also comply.

The key responsibilities Catch22 hold when acting as a Data Controller include:

1. Ensure compliance with the UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018 (DPA 2018), and the Privacy and Electronic Communications Regulations 2003 (PECR 2003).
2. Identification of a lawful basis for data processing
3. Data Processor Management
4. Implementation of appropriate technical and organisational measures
5. The handling of data subject right requests
6. Notification of Data Breaches to the ICO within 72 hours
7. Payment of the Data Protection Fee and registration with the ICO
8. Ensuring personal data is not retained for longer than is necessary
9. Ensuring only the minimum amount of personal data is processed as necessary for the purposes of processing
10. Ensure transparency of data processing for data subjects

These responsibilities are met and managed through their relevant processes, policies, assessments, templates, and agreements. Staff therefore **must** contact the DPO for sign off before starting any of the below:

- New Processing Operations
- High-Risk Processing (where processing may present a high risk to the individual)
- Implementation of new systems
- Review of any Data Processing, Data Sharing, and Joint Controller Agreements
- Legitimate Interest Assessments
- Data Protection Impact Assessments
- Updating of the Record of Processing Activities (ROPA)

Agreements

Catch22 services are regularly required to share personal data with other organisations including commissioners, public authorities, and private sector organisations. Relationships between organisations dictate the type of agreement required before data processing is to proceed. There are 3 relationships in relation to data sharing; Controller to Controller, Joint Controller, and Controller to Processor. The Data Protection Team hold templates for each of these 3 relationships:

Controller to Controller – Data Sharing Agreement
Joint Controller – Joint Controller Agreement
Controller to Processor – Data Processing Agreement

Where sharing of data will result in processing outside of the United Kingdom or European Economic Area (EEA), there are legal requirements for additional controls to be implemented. If any data is to be, or is currently being processed outside of the United Kingdom, it **must** be communicated with DPO@catch-22.org.uk.

6. Processing as a Data Processor

When acting as a Data Processor, we can legally only process personal data under the instructions of the Data Controller. These instructions are typically outlined in either a Data Processing Agreement or Data Processing Schedule that is included in an overarching contract. Our primary responsibilities include:

- Ensuring relevant security controls are implemented to protect data and systems
- Ensure staff are bound by confidentiality agreements
- Ensure all sub-processors are approved by the Data Controller before processing commences
- Support the Data Controller with data subject rights, incident response, and Data Protection Impact Assessment completion
- Restrict any further processing of data that would be outside the processing instructions unless authorised by the Data Controller
- Ensure secure deletion or return of data as outlined in the Data Processing Agreement or Schedule when processing is to end

Processing personal data outside of the instructions provided by the Data Controller results in Catch22 breaching both UK Data Protection Legislation and the contract between us and the Controller. Catch22 is then liable for potential reprimands and fines from the ICO and legal action from the Data Controller.

If a contract or agreement is provided by a Data Controller to Catch22 as a processor, it must be shared with DPO@catch-22.org.uk so it can be reviewed, adapted where required, and any risks raised prior to authorisation.

If processing instructions change, notify DPO@catch-22.org.uk for risk analysis and guidance. Keep all Data Processing Agreements, contracts, and Schedules securely

stored. The Data Protection Team will also retain any agreements, contracts, or schedules they receive.

As a minimum, Data Processing Agreements and Data Processing Schedules must include:

- The nature of processing to occur
- The purpose of the processing
- The types of data to be processed
- The categories of data subjects of which processed data will be about
- The duration of processing to be completed
- The retention timings of data to be processed
- The Data Controller's obligations and rights

7. Use of Sub-Processors

Sub-Processors are third parties that a Data Processor outsources processing activities to. This is typically an application provide or a contract delivery partner. There are two approval processes required for this to occur, the first being an internal approval process requiring the completion of a Data Protection Impact Assessment, updating of the Record of Processing Activity, and preparation for the release of an updated privacy notice with an updated consent form where applicable.

The second approval process sits with the Data Controller. All processing must be completed under the instructions of the Data Controller, this specifically includes engaging a sub-processor. It is a legal requirement under the UK GDPR that Data Processing Agreements, Contracts, or Schedules, include a clause outlining that specific or written authorisation from the Data Controller is required.

As the Data Processor, we are liable to the Data Controller for Sub-Processors compliance with Data Protection requirements. That means all sub-processors **must** go through mandatory due-diligence checks, ongoing monitoring of their processing activities, and management of any compliance risks. DPO@catch-22.org.uk can provide guidance where there are concerns around any sub-processors.

Where Catch22 need to change sub-processors, it is a legal requirement for us to notify Data Controllers and provide them the opportunity to object. In some cases, contracts will specifically require us to seek authorisation before changing sub-processors, review of service specific contracts is therefore mandatory before changes are implemented.

In any of the situations above, the Data Protection Team must be notified of planned changes to the sub-processors we use to ensure the relevant documentation and checks are completed.

8. Internal Processing Rules & Responsibilities

The rules for processing personal information are as below:

1. Staff must only process personal data for the approved purposes.
2. Staff must only use approved systems.
3. Where approved systems update to include Artificial Intelligence features, staff **must** make DPO@catch-22.org.uk aware.
4. Staff must not export data, create datasets, or repurpose data until it has been signed off by the DPO and authorisation received from the Data Controller. This does not apply if the original Data Processing Agreement or Contract include the specific tasks.
5. Staff **must not** introduce Shadow IT through the use of devices or systems not known or managed by the IT department.
6. Data Analytics and Data Sharing involving personal data **must not** be completed on personal data until it has been signed off by the Data Protection Team and where relevant, the Data Controller.
7. Where staff want to move data between business units, guidance **must** be sought from the Data Protection Team.
8. If staff become aware of any changes to processing activities, they **must** notify the Data Protection Team.
9. Where a data breach has been identified or processing has been found to deviate from the approved processes, staff **must** notify the Data Protection Team.

We all have responsibilities to ensure we areprocessing data appropriately and in compliance with UK Data Protection Legislation, these have been summarised below.

Managers

Managers must ensure teams follow approved operating procedures when handling personal data and do not deviate without requesting guidance from the Data Protection Team.

Where there are new or amended processing activities within a service or function, they must be submitted to DPO@catch-22.org.uk to ensure the relevant assessments are completed and documentation updated.

Managers must ensure all team members complete their Information Security and Data Protection awareness training. Where this has not been completed, managers are expected to be responsive to escalations regarding compliance gaps when received from the Data Protection or Information Security teams.

Managers must ensure all staff accept and complete their Data Protection policies via 4Policies. Where staff or managers are unsure on how to access these, guidance can be found on Catch Connect.

Staff

Staff have a responsibility to follow all documented operating procedures and to adhere to the confidentiality clauses agreed to within their employment contract.

All Data Protection incidents or breaches identified by staff must be reported immediately to the DPO via Datix.

Staff must only use approved systems and tools. Where new features have been added to an approved system or tool and data processing would be affected (an example would be a new AI feature), these must be reported to DPO@catch-22.org.uk before use.

Staff have a responsibility to complete all Information Security and Data Protection training. All policies must be accepted and quizzes completed where appropriate via 4Policies.

Staff must follow all service data retention, minimisation, and information security policies. In most cases, these are simply the overarching Catch22 policies.

Data Protection and Information Security Teams

The Data Protection Team hold the following responsibilities:

- Advise on new processing requests providing guidance to resolve any identified risks or areas of non-compliance.
- Review and sign-off Data Protection Impact Assessments providing DPIA codes once done (these codes are used to evidence completion and approval of DPIAs to other functions such as IT when requesting new applications).
- Provide guidance on Data Sharing Agreements, Data Processing Agreements, Legitimate Interest Assessments, Consent Form creation or updates, and Privacy Notice creation or updates.
- Review and provide guidance on all breaches submitted via Datix. This includes reporting of breaches to the ICO within 72 hours where it meets the threshold for reporting.

The Information Security team are responsible for:

- Ensuring adequate controls are implemented to protect the confidentiality, integrity, and availability of the data Catch22 processes and systems it is processed on.
- Ensuring Cyber Incidents are managed effectively through incident response plans minimising any impact on personal data.
- Ensure implemented controls are both internally and externally reviewed.

9. Use of Third Party Systems & Services

Third Party systems and services are used to enable the delivery of Catch22's services. These includes CRM systems, IT systems, and externally delivered services. To ensure data processing conducted while using these is legally compliant, assurance due diligence checks and reviews of service specific contracts are required. All data processing must strictly comply with service contracts so reviews **must** be completed

before the commencement of processing activities. Where a service is proposing the use of a new system which will process data, the Data Protection Team must be contacted at DPO@catch-22.org.uk.

In most cases, the use of third party systems or services result in the provider being a Data Processor. All service agreements **must** be sent to DPO@catch-22.org.uk for review and where necessary Data Processing Schedules are not in place, a separate Data Processing Agreement must be created and signed.

Third party systems can be very complex and in some cases, require data to be processed outside of the United Kingdom. Where this is the case, DPO@catch-22.org.uk **must** be made aware and a review of the relevant service's contract is to be reviewed to ensure data can be processed abroad. Where this is the case, specific contract requirements must be met, the Data Protection Team will advise where this is the case.

The Record of Processing Activity must always reflect data processing being conducted, if a new third party system or service is to be used, the relevant ROPA entry **must** be updated. This will typically be completed after the relevant DPIA has been signed off.

Features are continuously updated within technical systems, in some cases, this includes new Artificial Intelligence (AI) features. Where staff identify AI features being implemented into existing IT systems, it is important that DPO@catch-22.org.uk is notified so the required checks can be completed to ensure ongoing compliance with UK Data Protection Legislation.

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, 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.

11. Related policies

- Data Protection Policy Suite
- Information Security Policy Suite

12. Document Version Control

	Last Modified	Last Modified By	Changes Made
0.1	11/02/2026	Ben Wright	Policy draft rebuilt
1.0	13/04/2026	Ben Wright	Policy review completed and policy is live.

13. Annex 1: Equality Impact Assessment

Summary

This EIA is for:	DP 07 Data Processing 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 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?	☒	☐	☐	
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 policy applies equally to all individuals whose personal data is processed by Catch22, including service users, staff, and other stakeholders.

- Requests may be made through multiple channels, reducing barriers for individuals who may otherwise be disadvantaged.
- Where identity verification or clarification is required, this will be carried out proportionately and with sensitivity to individual circumstances.
- No negative equality impacts have been identified. The policy is considered to have an overall positive impact by enabling individuals to exercise their statutory rights fairly and consistently.