# Catch22 group policy

*Data Protection – Subject Access Request 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: | *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* |

# Document Version Control & Changes

| Version | Last modified | By | Changes Made |
|---|---|---|---|
| 1.0 | 30/06/2022 | Beverley Clark | Updated policy in line with UK Data Protection Legislation |
| 1.0 | 30/06/2023 | Beverley Clark | Policy reviewed; no changes made. |
| | | | |
| | | | |

## Catch22 GDPR 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. Summary

The United Kingdom General Data Protection Regulation (UKGDPR) affords data subjects 10 rights, one of which is the right of access. Data subjects/individual(s) have the right to access their personal data from a data controller who is processing their data. This policy outlines Catch22's commitment to this right and highlights the process that is followed to ensure that access requests are dealt with in a timely fashion.

### 2. Policy statement

Catch22 will take all reasonable actions to ensure that it is compliant with Article 15 of the Regulation, that:

*"The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data..."* and *"The controller shall provide a copy of the personal data undergoing processing."*

In the event that a data subject makes a request to access the data held about them by Catch22, we will respond to that request, subject to verification of identity, within one month of the request. If this is not possible, we will provide the data that is available within that time and advise the requestor that we need additional time with a clear indication of the timeframe that we expect to be able to fulfil their request within.

## 3. Policy requirements

### a. Upon receipt of data subject access request (DSAR)

Upon receiving a request staff are required to report this to the Data Protection Officer at dpo@catch-22.org.uk immediately. The DPO will work with relevant staff to:

- Verify whether Catch22 hold the data subject's personal data. If Catch22 is not the controller, but merely a processor, inform the data subject and refer them to the controller. Catch22 will ensure that we support the controller promptly with any data that we hold on their behalf;
- Verify the identity of the data subject; if needed, request any further evidence on the identity of the data subject.
- Verity the access request; is it sufficiently substantiated? Is it clear what information is requested? If not: request additional information.
- Verify whether request(s) are unfounded or excessive (in particular because of their repetitive character); if so, Catch22 may refuse to act on the request or charge a reasonable fee.
- Promptly acknowledge receipt of the SAR and inform the data subject of any costs involved in the processing of the SAR
- Verify whether you process the data requested. If you do not process any data, inform the data subject accordingly. At all times make sure this policy is followed and progress can be monitored.

- Ensure data will not be changed as a result of the SAR. Routine changes as part of the processing activities concerned are permitted.
- Verify whether the data requested also involves data on other data subjects and make sure this data is redacted before the requested data is supplied to the data subject; if data cannot be redacted, ensure that other data subjects have consented to the supply of their data as part of the SAR or unless it is reasonable to disclose without the other person's consent.

**Charging a fee for requests**

Fees can only be charged to the requester in two distinct instances, when the request is manifestly unfounded, excessive or repetitive or when there is a request for further copies of the same information. Unless these two scenarios apply, the information must be provided free of charge. For further detail on charging fees please contact the DPO for guidance.

**b. Responding to DSAR**

In addition to providing the requester with their personal data, controllers are also required to provide them with the following information:

- The purpose of the processing
- The categories of the personal data concerned
- The recipients or categories of recipient to whom the personal data have been or will be, disclosed, in particular recipients in third countries or international organisations
- Where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period
- The existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing
- The right to lodge a complaint with the Information Commissioners Office
- Where the personal data are not collected from the data subject, any available information as to their source

- The existence of automated decision-making, including profiling and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Data can be provided in both electronic and written format, depending on the requester's preference and the viability of producing the data in that format. The requester's data will be provided to them without **undue delay and within one calendar month** of the receipt of the request. This time period may be extended by an additional two further months, where necessary, taking into account the complexity and the number of requests. In instances where the organisation elects to extend the deadline, DPO's will inform the requester of the extension and the reasons why the extension was taken.

## 4. Definitions

**Personal data** means data which relate to a living individual who can be identified either directly or indirectly –

(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 controller** means … a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.

A data controller must be a "person" recognised in law, that is to say:

- individuals;
- organisations; and
- other corporate and unincorporated bodies of persons.

Data controllers will usually be organisations, but can be individuals, for example self-employed consultants. Even if an individual is given responsibility for data protection in an organisation, they will be acting on behalf of the organisation, which will be the data controller.

In relation to data controllers, the term jointly is used where two or more persons (usually organisations) act together to decide the purpose and manner of any data processing. The term in common applies where two or more persons share a pool of personal data that they process independently of each other.

**Data processor**, in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.

Data controllers remain responsible for ensuring their processing complies with the Act, whether they do it in-house or engage a data processor. Where roles and responsibilities are unclear, they will need to be clarified to ensure that personal data is processed in accordance with the data protection principles.

A person is only a data controller if, alone or with others, they "determine the purposes for which and the manner in which any personal data are processed". In essence, this means that the data controller is the person who decides how and why personal data is processed.

**Inaccurate data,** data are inaccurate if they are incorrect or misleading as to any matter of fact.

Personal data may not be inaccurate if it faithfully represents someone's opinion about an individual, even if the opinion proves incorrect (for example, a doctor's medical opinion about an

individual's condition). In these circumstances, the data would not need to be "corrected", but the data controller may have to add a note stating that the data subject disagrees with the opinion.

**Recipient,** in relation to personal data, means any person to whom the data are disclosed, including any person (such as an employee or agent of the data controller, a data processor or an employee or agent of a data processor) to whom they are disclosed in the course of processing the data for the data controller, but does not include any person to whom disclosure is or may be made as a result of, or with a view to, a particular inquiry by or on behalf of that person made in the exercise of any power conferred by law.

**Third party**, in relation to personal data, means any person other than –

(a) the data subject,

(b) the data controller, or

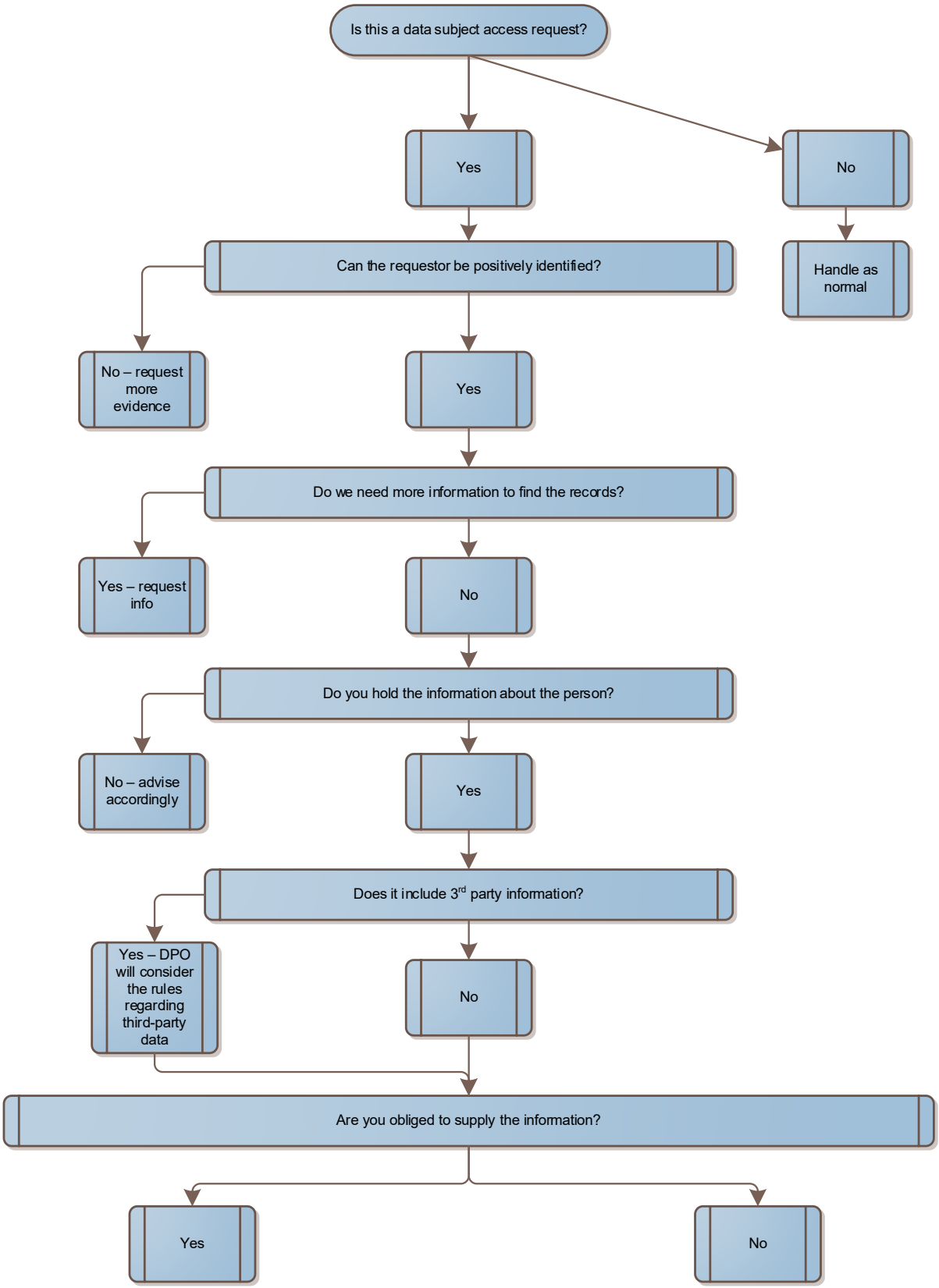
(c) any data processor or other person authorised to process data for the data controller or processor.

## 5. Related policies

Data Protection Policy Suite

ISO 27001 Policy Suite

## 6. Data subject access request flowchart



# Annex 1: Equality Impact Assessment

## 1. Summary

| | |
|---|---|
| **This EIA is for:** | Data protection: Subject access request policy – January 2021 |
| **EIA completed by:** | Beverley Clark, Data Protection Officer |
| **Date of assessment:** | 30 June 2022 |
| **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**<br>Does this policy impact on any particular age groups or people of a certain age? | ☐ | ☒ | ☐ | |
| **Disability**<br>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)**<br>Does this policy impact on people who are transitioning from one gender to another (at any stage) | ☐ | ☒ | ☐ | |
| **Marriage and civil partnership**<br>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)**<br>Does this policy impact on people who are pregnant or in their maternity period following the birth of their child? | ☐ | ☒ | ☐ | |
| **Race**<br>Does this policy impact on people as defined by their race, colour and nationality (including citizenship) ethnic or national origins | ☐ | ☒ | ☐ | |

| | | | | |
|---|---|---|---|---|
| **Religion and belief**<br><br>Does this policy impact on people who practice a particular religion or none, or who hold particular religious or philosophical belief or none? | ☐ | ☒ | ☐ | |
| **Sex**<br><br>Does this policy impact on people because they are male or female? | ☐ | ☒ | ☐ | |
| **Sexual orientation**<br><br>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.** |
|---|
| |