Catch22 group policy

Data Protection – Consent to process data 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 – no changes
2.0	26/06/2023	Beverley Clark	Policy review – no changes
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	Policy review – no changes

Catch22 UKGDPR standards

When processing personal data staff will uphold the following standards:

- **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 six 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

The United Kingdom General Data Protection Regulation (UKGDPR) and Data Protection Act 2018 specify six lawful ways in which personal data can be processed. Catch22 will cite a number of these to justify and legitimise it's processing of personal/special category data. Historically one of the more commonly used legal basis, that is cited, is that of the data subject's explicit consent. Consent is defined under the UKGDPR as 'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or clear affirmative action, signifies agreement to the processing of personal data relating to him or her'. This policy will highlight Catch22's approach if and when consent is deemed to be the most suitable appropriate lawful basis in which to process personal data.

2. Scope

As and when consent has been identified as an appropriate lawful basis for processing (please see the ICO's lawful basis interactive guidance tool for further help for identifying the appropriate lawful basis for processing - https://ico.org.uk/for-organisations/gdpr-resources/lawful-basis-interactive-guidance-tool/) it is essential that consent is gathered in the correct way in order to ensure compliance with the law. Furthermore, if consent is addressed correctly it can enhance the individuals experience and give them confidence that we will treat them and their data with care.

The aim of this policy is to ensure that all staff are aware of requirements in relation to using consent as a means to justify data processing.

3. Consent checklist

In relation to the requesting, recording and managing of consent, Catch22 will:-

- **c**heck that consent is the most appropriate lawful basis for processing
- make the request for consent prominent and separate from other terms and conditions
- ask people to positively opt in
- not use pre-ticked boxes or any other type of default consent

- use clear, plain language that is easy to understand
- specify why we want the data and what we're going to do with it
- give individuals options to consent separately to different purposes and types of processing
- name our organisation and any third party controllers who will be relying on the consent
- tell individuals they can withdraw their consent
- ensure that individuals can refuse to consent without detriment
- avoid making consent a precondition of a service
- keep a record of when and how we got consent from the individual
- keep a record of exactly what they were told at the time
- regularly review consents to check that the relationship, the processing and the purposes have not changed
- have processes in place to refresh consent at appropriate intervals, including any parental consents
- consider using privacy dashboards or other preference-management tools as a matter of good practice
- make it easy for individuals to withdraw their consent at any time, and publicise how to do so
- act on withdrawals of consent as soon as it can
- not penalise individuals who wish to withdraw their consent

➔ **Freely given**

One of the requirements of consent is that it is freely given. This means that consent can only be provided where there is **not** a clear imbalance between the individual and Catch22. Freely given indicates that the individual must not be under any pressure or duress to provide consent and they must have a choice about whether to consent or not without the consequence of withholding consent being to their detriment. This means that it will rarely be appropriate for consent to be used as the basis for processing data in a service context.

Scenario: a young person is referred to our service for support. As part of the referral they have agreed for their details to be passed to us for the purpose of us providing them with support to achieve agreed outcomes.
Our contract with the commissioner (data controller) requires us to collect certain information about the person including personal information, type of support accessed, whether the support was accepted or rejected, outcomes achieved.
In this case, if we relied solely on consent to process the service users data, in the event that they withdrew their consent to us doing that, we would not be able to report back to the commissioner against our contractual requirements. Consent to process data in this case therefore does not work and we have to rely on one of the other conditions for processing to carry out our role – in this case it would be "for the performance of a contract to which the data subject is party".

Another example where consent would not be considered to be freely given, would be when People Services are collecting staff data. It is clear that Catch22 has a legitimate/legal need to hold/process staff information and therefore consent would not be an appropriate means of processing this information.

➔ **Specific**

Consent will also need to be specific to the proposed processing and be obtained in a way that is distinguishable from other matters. It must cover all processing activities carried out for the same purpose or purposes and where processing has multiple purposes, consent must be given for all of them.

➔ **Informed and unambiguous**

Individuals (data subjects) need to be made aware of exactly what will be done with their data if the consent to the proposed processing. This information will need to be provided to the data subject in the form of a privacy notice (please see privacy notice briefing paper for further detail). The GDPR specifies the key pieces of information that will need to be provided to data subjects to ensure that they are well informed about the processing, for example:

- the identity and the contact details of the controller,
- the contact details of the data protection officer,
- the purposes of the processing for which the personal data are intended as well as detailing that the lawful basis for processing their data is through consent;
- the recipients or categories of recipients of the personal data, if any;
- where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation.

In addition, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
- the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- the right to lodge a complaint with a supervisory authority;
- the existence of automated decision-making, including profiling, 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.

➔ **Demonstrable**

The UKGDPR specifies that the controller must not only gather consent, it must also be able to demonstrate that the data subject has consented to processing of his data, meaning that records will need to be kept for consent to be verifiable. This will need to be dated to

ensure that there is a record of when the data subject consented to the proposed processing.

➔ **Consent may not be the most appropriate basis for processing**

Historically consent has been seen as the gold standard with regard to justifying data processing. In many cases consent is used but is not the most appropriate legal basis for processing. There are 5 other legal basis for processing that can be utilised and may be more appropriate to the processing activity. The other legal basis that can be used are;

- *Performance of contract*
- *Legal obligations*
- *Vital interests*
- *Public interest/execution of a public authority*
- *Legitimate interests*

***As an organisation we should not be relying upon consent unless it is absolutely necessary*.** Consent should generally only be used for non-business as usual processing such as marketing where individuals are able to rescind their consent at any time. Please contact the DPO in instances where you are unsure what legal basis could apply to the processing activity.

4. Definitions

For definitions please see the Data Protection: Over-arching Policy 2018.

5. Related policies

Data Protection Policy Suite

Annex 1: Equality Impact Assessment

1. Summary

This EIA is for:	Data protection: Consent to process data policy
EIA completed by:	Beverley Clark, Data Governance Manager
Date of assessment:	11 January 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?	☒	☐	☐	The policy sets out the framework for consent including consent conditions that apply to under 13s which is the UK age for GDPR consent – guidance below.
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.
https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid-consent/ Guidance on age appropriate consent.