Catch22 group policy

Data Protection – Over-arching 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
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 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 it holds in the course of doing business with the highest care and respect. In order to do this we will abide by a number of principles which are based on, but not limited to, the United Kingdom General Data Protection Regulation (UKGDPR), the Data Protection Act 2018, the Privacy & Electronic Communications Regulation (EC Directive) Regulations 2003 (PECR), ePrivacy Regulation and the Human Rights Act 1998.

We understand the responsibility that we hold and trust that is placed in us in holding the personal information of our staff, volunteers, service users, contractors, stakeholders, supporters and other individuals who in the course of our business provide us with their relevant personal information. We will ensure that we implement the appropriate organisational and technological measures to protect the information as required based on the level of assessed risk for each data asset.

2. Scope

The aim of this policy is to ensure all staff are aware of their responsibilities and obligations in relation to data protection in order to minimise risk of infringement. The policy also aims to improve the understanding of the asset value of the data Catch22 holds. It aims also to inform members of the public how Catch22 complies with data protection legislation and how to exercise their rights to the data we hold about them.

3. 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 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 genetic or biometric data processed solely to identify a human being

(f) their physical or mental health or condition,

(g) their sexual life,

(h) the commission or alleged commission by them of any offence, or

(i) 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.

4. Legal Basis

- Data Protection Act 1998
- UK General Data Protection Regulation

- Privacy & Electronic Communications Regulation 2003
- Data Protection Act 2018
- Human Rights Act 1998 (in particular Article 8)
- (ePrivacy Regulation – currently in draft stage)

5. Statement of principles

Catch22 will: -

- ensure that anyone whose data is processed is provided with a clear and unambiguous notice detailing what information we hold, why we hold it, who it is shared with and for what purpose, how long it will be held for, who the data controller is and how to contact them and how to exercise their rights;
- respond to information rights requests in a timely and appropriate way including
    - access (subject access request)
    - deletion (right to be forgotten)
    - rectification
    - restriction of processing
    - data portability
    - objection
- implement the appropriate organisational and technological security measures to protect the data we hold based on the level of assessed risk of the data assets held;
- only collect the information that is needed for the purpose specified (data minimisation)
- ensure that the data we hold is accurate, necessary, updated where required and relevant to the purpose for which it was collected;
- ensure that information is only accessible to those people who are required to have access to it (least privilege)
- only keep data for as long as necessary;
- ensure that any new service or method of working is suitably assessed for privacy and information risks (data protection impact assessments);
- build privacy into the design of any new service or method of working as a starting point (privacy by design, privacy by default)
- appoint a data protection officer to ensure that the organisation is kept aware of its responsibilities under the law, including maintaining and updating the registration with the ICO, and to provide support to all those who process data in the organisation.

6. Responsibilities

Data protection is the responsibility of each and every member of staff in Catch22. Whilst the data protection officer is the named lead in the organisation, every person who works for Catch22 is responsible for ensuring that information is held appropriately, securely and

treated with respect.

Individual members of staff are responsible for ensuring they act within the scope of the law, and seek further advice firstly from the Governance Team where necessary.

7. 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.

8. Breach of policy

Breach of data protection law may render both the Board of Trustees and/or individuals liable to both civil enforcement and/or criminal proceedings. Catch22 will regard wilful or reckless breach of this policy and its associated policies as a disciplinary offence and such breaches will be subject to Catch22's disciplinary procedures.

9. Review

This policy will be reviewed every two years or on an ad hoc basis as necessary

10. Related policies

- Data Protection Policy Suite
- ISO 27001 Policy Suite

Annex 1: Equality Impact Assessment

1. Summary

This EIA is for:	Data protection: Over-arching policy
EIA completed by:	Beverley Clark, Data Governance Manager
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 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.