Catch22 group policy

Data Protection – Data incident policy

Contents

1. Summary 3
2. Policy statement 3
3. Internal reporting requirements 4
4. External reporting requirements 4
    i. Notification of breach to the ICO
    ii. Notification of breach to the individual(s) affected
5. Definitions 6
6. Related policies 7
7. Appendices 8
    a. Data reporting flowchart 8
    b. Data Protection Incident form 9

Annex 1 – Equality Impact Assessment 14

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

Policy Owner:	*Governance & Risk*
Queries to:	*Data Governance Manager*
Date created:	*31 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*

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 GDPR are upheld appropriately and in accordance with the regulation and associated legislation.

- **Accountability**

  Staff will adhere to and remain compliant with the seven GDPR 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

Catch22 processes large amounts of personal/special category data which is a valuable asset and integral to the smooth running of the organisation. Every care is taken to ensure **that this data is processed securely using appropriate technical and organisational measures** and processed in compliance with the GDPR and Data Protection Act 2018 (DPA). Compromise of personal data, confidentiality, integrity, or availability may result in harm to individual(s), reputational damage, detrimental effect on business as usual, legislative non-compliance and or financial costs.

2. Policy statement

Catch22 will take all reasonable actions to ensure that it is compliant with Article 5.1.f of the Regulation:

"*Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technological or organisational measures ('integrity and confidentiality').*"

In the event of a breach, Article 33 requires that the Controller inform the Information Commissioner within 72 hours of becoming aware of the issue. Catch22 will implement the following procedure to ensure that data breaches that do occur are contained, mitigated and reported in accordance with regulatory requirements in order to minimise the adverse effects on the organisation and on the individuals affected.

3. Internal reporting requirements

In the event that the security and confidentiality of personal/special category data is compromised we will act immediately to limit any potential impact on individuals and to review and improve our own arrangements. The Data Protection Officer (DPO) plus the line manager and relevant director must be notified of any breach/data loss as soon as it has been identified to ensure that we are able to report the breach to the Information Commissioners Office (ICO) and the data subject(s) as soon as possible, if the breach is significant. Acting promptly will allow for measures to be implemented to mitigate and contain the breach, reducing the effect on the individuals affected and to the organisation.

With the exception of the Catch22 MAT schools, all other services must complete an information security report on Datix. Please click the link and select your hub, you will automatically be taken to the appropriate page. Reporting a Data Breach

4. External reporting requirements

a. Notification of breach to the ICO

Catch22 as a data controller is required by law to notify the ICO of a breach of personal data without undue delay and where feasible no later than 72 hours after having become aware of it, where the breach is likely to result in in a risk to the rights and freedoms of the individual(s) affected.

Once the breach has been escalated to DPO's, line manager and relevant director, DPO's and other key stakeholders will make a judgement as to the severity of the data breach and implement any actions that can be taken to contain and mitigate the adverse effects of the breach. If it is deemed that the breach is significant and is likely to result in a risk to the rights and freedoms of the individual(s) affected, they will report the breach to the ICO immediately. Only Catch22's DPO's should contact the ICO in these instances.

The report to the ICO will include the following information:

- description of the nature of the personal data breach including, where possible, the categories and approximate number of individuals concerned and the categories and approximate number of personal data records concerned;
- the name and contact details of Catch22's DPO's;

- description of the likely consequences of the personal data breach;
- description of the measures taken or proposed to be taken to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

b. Notification of breach to the individual(s) affected

In addition to the requirement to notify the ICO there is also a legal requirement to inform the individual(s) that are affected, that their data has been compromised in a breach. Again this requirement is weighted by whether there is a high risk to the rights and freedoms of the individual(s) involved. As with the requirement to notify the regulator DPO's and other key stakeholders will make a decision as to the impact of the breach and whether the individual(s) will need to be notified.

The report to the data subject(s) will include the following information:

- the name and contact details of Catch22's DPO's;
- description of the likely consequences of the personal data breach;
- description of the measures taken or proposed to be taken to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Catch22 is not required to inform data subject(s) of the breach if any of the following conditions are met:

- Catch22 has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
- Catch22 has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects of data subjects is no longer likely to materialise;
- it would involve disproportionate effort. In such case there shall instead be a public communication or similar measures whereby the data subject(s) are informed in an equally effective manner.

Regardless of the severity of the breach and the obligation to report the breach to the ICO/data subject(s), DPO's will ensure that the following actions are carried out following a breach:

- an investigation of the circumstances of the breach

- a report to be completed by the service manager detailing the circumstances of the breach with a risk assessment focussing on the potential impact of the loss for individuals and identifying mitigating action to reduce the risk where possible
- the implementation of an action plan with local and organisational actions to improve our procedures
- a review of the Policy, Guidance and any other related material or resources in the light of the incident
- dissemination of the learning through communication methods as appropriate.

5. 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 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.

For all other definitions please see the Data Protection: Over-arching Policy 2020.

6. Related policies

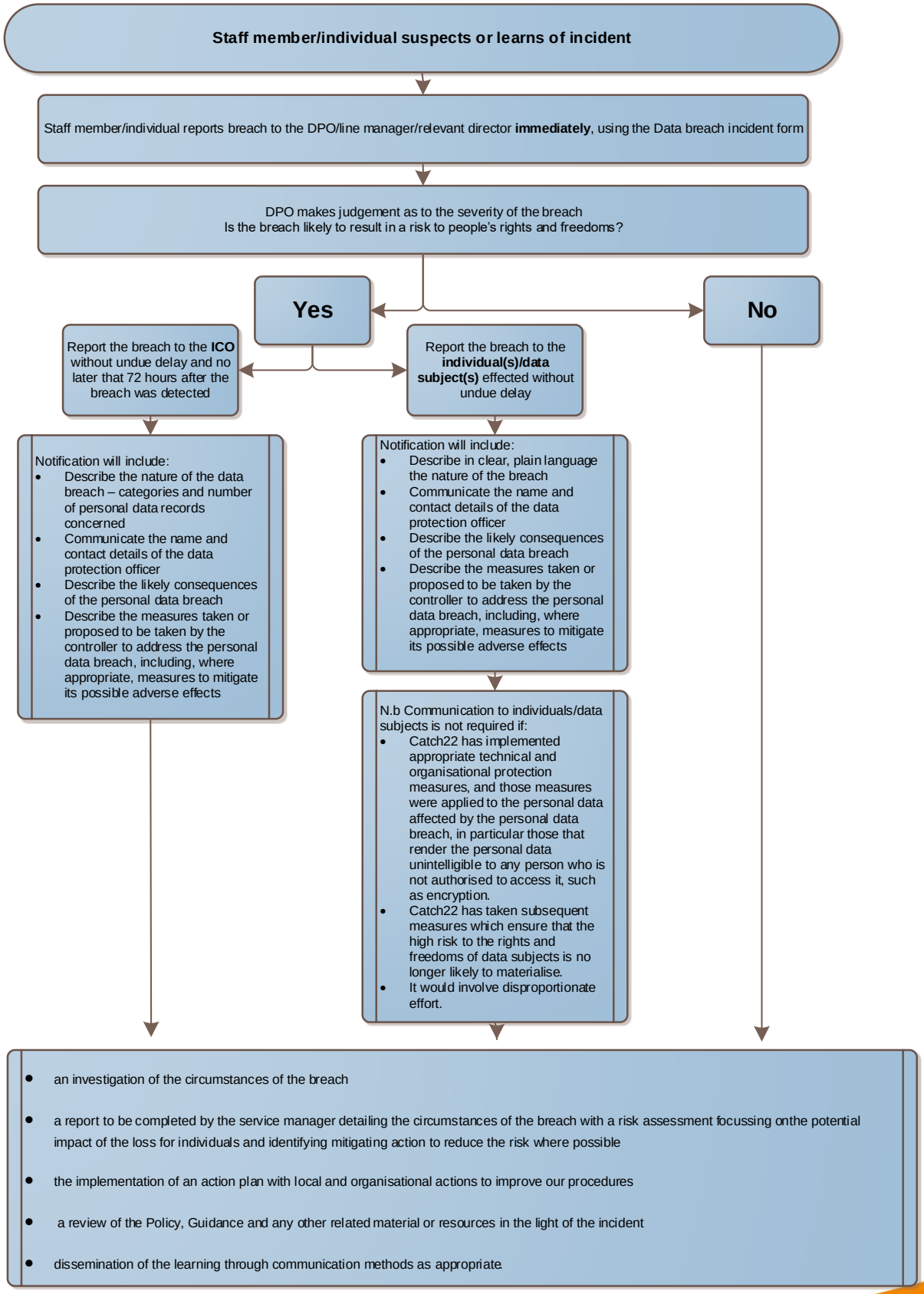
Data Protection Policy Suite
ISO 27001 Policy SUite

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 – Datix link added.

7. Appendices

Data reporting flowchart

Data/information security incident form



For Catch22 MAT Schools only

Data/Information Security Breach Form
Part 1 – Incident Details

*(This form must be completed and sent on to the Data Protection Officer **dpo@catch-22.org.uk** as soon as an incident has been identified. Copies must also be sent to your Line Manager and Director or Education CEO)*

A. Details of Person completing the form			
Full Name			
Job Title			
Service name/Location			
Contact number			
Business area Highlight	Apprenticeships Community Links Corporate Education – Independent schools Education – MAT Employability Justice	Launch22 Lighthouse NCS Only Connect Unlocked Vocational training – colleges YP & F	Other – please specify….
Date and time the incident **occurred**:	DD/MM/YYYY HH:MM		
Date and time the incident was **discovered**:	DD/MM/YYYY HH:MM		
Date and time of the incident **reported** to DPO/Manager:	DD/MM/YYYY HH:MM		

B. What information/data has been lost/shared inappropriately?	
Please include: - Type of information – please give generic details of the information lost/shared inappropriately i.e. name, date of birth, address, case notes, medical reports, offending history or reports etc.	

C. Details of incident	
Description of Incident: Please ensure that you include how the incident occurred, who was responsible for the data at the time, what actions were taken at the time to recover the loss, any indication that the data has been used by an unauthorised person etc. who has been informed	

D. What were your immediate actions following the incident?	
Description of actions taken directly after the incident	

E. Further details					
Who is the Data Controller (owner) of this data? (See relevant contract if unsure)	Catch22 ☐ Other ☐ Please specify:		If Catch22 is not the Data Controller, has the Data Controller been made aware of the incident? Yes ☐ No ☐		
How the information was stored	Paper/File ☐	Laptop ☐	USB data stick or other portable storage device ☐	Smartphone or Smartpad eg I-pad etc ☐	Other ☐ Please specify:
If IT or Comms equipment was it encrypted?	Yes ☐ Please give detail:		No ☐ Please give detail:		
Was the data password protected?	Yes ☐ Please give detail:		No ☐ Please give detail:		
Number of people affected/potentially affected					
Approximate number of personal data records concerned					
Group(s) affected	Service users ☐	Staff ☐	Volunteers ☐	Partners ☐	Other ☐ Please specify:

Sensitivity type	Personal ☐	Sensitive (Special Category) ☐	Commercially sensitive ☐	Criminal conviction and offences ☐	Other ☐ Please specify:
Sensitivity level	High ☐	Moderate ☐	Low ☐	Negligible ☐	
Reported to Line Manager:	Yes ☐	No ☐			
Reported to Director:	Yes ☐	No ☐			

Remember to **password protect** this document with password prior to sending

Part 2 – Management Review, Action Plan & Follow Up

(This section of the form is designed to aid managers to think through the issues that led to, or arose from, the incident and to identify any actions or follow up work that may be required)

F. Investigation completed by:			
Name		Job Title	
Location		Date	

Progress:			
Conclusion:			
Lessons learnt:			
Action taken/to be taken to prevent reoccurrence: i.e. training, updating processes			
Signed by manager:		Date:	DD/MM/YYYY

Remember to **password protect** this document with password prior to sending

Part 3 – DPO Review

G. Additional DPO comments (for completion by Data Protection Officer):		
Is the incident a data breach?	Yes ☐	No ☐
If so, is the breach internally reportable?	Yes ☐	No ☐
Have the following parties been made aware of the incident?	Information Commissioner's Office Yes ☐ No ☐ If reported, please give name of the person spoken to, contact number and role:	Data subject(s) Yes ☐ No ☐ If contacted, please give name(s) of the person(s) spoken to:
	Date/time reported: DD/MM/YYYY HH:MM	Date/time contacted: DD/MM/YYYY HH:MM
Was incident reported to DPO as soon as staff became aware?	Yes ☐	No ☐ Reason for delay?

H. DPO review:			
Document reasoning around decision made to report/not to report to ICO/data subjects:			
Lessons learnt: - what might have been done differently - what learning has there been for the service and for Catch22/partners			
Signed by DPO:		Date:	DD/MM/YYYY

Annex 1: Equality Impact Assessment

1. Summary

This EIA is for:	Data protection: data incident policy – June 2020
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 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.