

Catch22 policy

Business Continuity

Contents	Page
1. Introduction	3
2. Purpose	3
3. Scope	3
4. Policy statement	4
5. Benefits	5
6. Ensuring continuity – a summary of action	5
7. Related policies	8
8. Business Continuity Plan Template	9
Annex 1 – Equality Impact Assessment	22

Policy owner	Director of Governance, Risk & Compliance
Queries to be directed to:	Director of Governance, Risk & Compliance

This policy will be reviewed on an annual basis.

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

Date created:	July 2009
Date of last review:	April 2026
Date of next review:	April 2027

Document Version Control & Changes

Version	Last modified	By	Changes Made
1.0	01/10/2021	Nigel Richards	Annual Review – no changes
1.1	01/04/2023	Nick Thatcher	Annual Review – changes to page
1.2	01/09/2024	Nick Thatcher	Annual Review – changes to page
1.3	23/04/2025	Nick Thatcher	Annual Review – changes made contents page
1.4	25/03/2026	Nick Thatcher	Annual Review -

1. Introduction

This policy outlines the scope and approach to business continuity management (BCM) within Catch22. For the purpose of this policy, business continuity is defined as a framework for creating and improving resilience and which will enable Catch22 to continue to deliver an acceptable level of service of its critical activities in the event of any unexpected disruption.

2. Purpose

As a social business and a supplier of services to local and national government, Catch22 is required to align with standards that these commissioning authorities work to including, but not limited to, the Security Policy Framework, (SPF) and ISO 22301. Under the Mandatory Requirement 70 of the SPF, Catch22 “must have robust, up to date, fit for purpose and flexible business continuity management arrangements that are regularly tested and reviewed and supported by competent staff that allow them to maintain, or as soon as possible resume provision of, key products and services in the event of disruption”.

ISO 22301 states that, “Top management shall establish and demonstrate commitment to a business continuity policy. The policy shall make reference to:

- a) the organisation’s business continuity objectives; and
- b) the scope of business continuity, including limitations and exclusions

The policy shall be:

- a) Approved by top management;
- b) Communicated to all persons working for and on behalf of the organisation; and
- c) Reviewed at planned intervals and when significant changes occur.”

The aim of this policy is to ensure that the appropriate business continuity management system framework is in place within each department/service so that it can meet these requirements and, by doing so,

- Reduce the risk of interruption or negative impact on delivery to key business services;
- Minimise disruption and enable full restoration of services within locally agreed recovery time objectives;
- Ensure that business continuity management principles are embedded in the daily operational activities and culture of the organisation.

3. Scope

This policy will apply to all aspects of Catch22, which, in addition to all corporate and office based activities will include:

- Schools;

- Prisons;
- Staff based at home;
- Staff based at remote or 3rd party locations;
- All external facilities, suppliers, contractors and third parties that the organisation/services rely upon for business services and products.

4. Policy statement

The organisation's corporate services business groups, frontline services and any other offices will develop, implement and maintain their own risk based business continuity plans and will ensure that they identify:

- Key internal staff, business critical activities, systems and services;
- Key external contacts and emergency contact points;
- Any internal or external service dependencies;
- The risks associated with those dependencies and how they can be addressed;
- Recovery time objectives;
- Potential fall-back options in the event of denial of access to buildings;
- Out of hours contact arrangements.

All business continuity plans must be owned and signed off by a senior member of the relevant operational or corporate support management team (minimum Assistant Director/Head of Service or above) who will be responsible for ensuring that:

- Plans are maintained and provide an ongoing capability for responding to unexpected incidents;
- A programme is in place to ensure plans are regularly tested and reviewed, (at least annually);
- The necessary in-house resource and expertise are provided to develop, implement and manage the plan, as well as post incident recovery;
- Staff are made aware of the BCM process and that those with business continuity roles receive regular training;
- Roles and responsibilities are clearly defined within the plan;
- Plans contain a risk-based business impact analysis that identifies all critical activities and time sensitive business objectives, key suppliers and interdependencies;
- That key suppliers or business partners which support a critical activity have effective BCM arrangements in place and can evidence this;
- A business continuity coordinator/practitioner is appointed to liaise with
- The Critical Incident Team should be informed by the Hub SLT in the event of a suspected critical incident. See Critical Incident Management Policy for more details.

Arrangements will be developed to independently audit BCM governance processes at regular intervals (at least annually) to ensure that they are fit for purpose.

5. Benefits

This policy is designed to provide a clear commitment by Catch22 to business continuity management across the whole organisation. Effective business continuity will enable Catch22, its partners, suppliers and affiliates to:

- Continue to provide critical services to service users, the public, business partners and other stakeholders during unexpected incidents;
- Minimise disruption and enable full restoration of services in the event of an incident;
- Comply with accepted standards of corporate governance;
- Reduce the operational and financial impact of any period of disruption;
- Ensure that all key personnel are identified and made aware of their responsibilities in regard to any recovery procedure;
- Improve the resilience of the organisation's infrastructure to reduce the likelihood of disruption; and,
- Ensure that the business continuity management structure is embedded in the day-to-day operational activities and culture of the business.

6. Ensuring continuity – a summary of action

IT Systems - Catch22 recognises the increasing importance of IT systems to the successful delivery of our business; particularly a reliance on email communication and data management software.

To ensure the security and continuity of our IT systems Catch22 will require any third party IT supplier to provide us with a system resilience and disaster recovery plan that includes a full risk and impact assessment, details of any dependencies and fail over arrangements, target recovery times and out of hours arrangements.

As a minimum standard Catch22 will ensure the following measures are implemented and maintained:

Hybrid Cloud data solution

- Replication of data to an off-site co-location, facilitating the restoration of data if required.
- Backups made to tape and sent off-site at regular intervals. For long term storage
- A hybrid Cloud solution that replicates both off-site data centres with instant fail-over.
- In the event of a physical disaster, servers can be brought up in a co-location data centre.
- High availability O365 systems which keep both the data and system replicated off-site, enabling continuous access to systems and data, even after a disaster.
- UPS and back-up generator to keep systems going in the event of a power failure for sensitive equipment.

- Core backbone internet for private cloud infrastructure.
- Wanstor as the managed service provider will be the main point of contact for recovery to be carried out.

Local site setups

- Azure domain-joined devices using MS OneDrive, TEAMS and SharePoint apps to store, backup and protect company data.
- Surge protectors — to minimize the effect of power surges on delicate electronic equipment.
- UPS to keep systems going in the event of a power failure for sensitive equipment.
- Fire prevention/mitigation systems such as alarms and fire extinguishers.
- Anti-virus software and other security measures.
- Access to 5G modems or mobile tethering for failover in the event of internet-related outages.

In the event of core infrastructure communications failure, alternative (off band/out-of-band) communications will be utilised e.g. WhatsApp, mobile phone and face to face contact.

Disease Epidemics/Pandemics - Catch22 have recognised the possible impact of a disease / flu / infectious disease epidemic or pandemic as potentially drastically reducing a healthy work force and placing significant strain and change on working arrangements. In order to ensure that Catch22 can minimise the risk of infection to our work force, and reduce potential disruption to our services some basic criteria have been identified:

- Awareness of World Health Organisation & Government controls in the case of an epidemic or a pandemic - first and foremost to realise the importance of complying with these control measures to minimise the risk to the larger population and health of our own workforce. In the most extreme cases we recognise that we would unavoidably have to shut our premises / sites down if instructed and facilitate alternative working arrangements (e.g. working from home) as permitted or advised by Government or other lead agency.
- Education of the staff base – an agreed percentage of staff will be trained in first aid to ensure that they are aware of the basics involving the transfer of disease / infections.
- Local safeguards - all managers will ensure that wash areas are kept clean and available at all times and that any repairs or re-charging of soap or hand towel dispensers is carried out as a priority
- Monitoring of direct & subcontract staff, volunteers and service users in the incident of a possible outbreak - if the Government raises the possibility of an epidemic or pandemic all managers will be instructed to monitor all those present for signs of infection and to send them home where there is a relevant case and notify the H&S team. In these circumstances managers will ensure that a report is sent immediately to the H&S team and that all due precautions are taken to avoid further infection/contamination. Any

guidance from the World Health Organisation or the Chief Medical Officer of Great Britain will be disseminated widely using all communications systems available as required.

- Ability to work remotely / at home – where work does not have to be carried out in the office, staff can access documents / email from home-based computers, meaning that even if a site cannot open, information exchange can continue, and core administrative activities can be undertaken remotely.
- Details of local and national key contacts and emergency contact points to be available and accessible for the management and monitoring of any actual or suspected infectious disease incident

Natural Disasters / Extreme Weather / Fire - Catch22 recognises that such events are likely to be localised, notwithstanding the effects of flooding which can cover wide geographical areas.

In such an event our priority will be to ensure the safety of our workforce and the general public (if affected) through co-ordination with the relevant emergency services. Once we are satisfied that all parties are safe and the disaster / event is over we will aim to assess the damage to our sites / business premises as soon as possible and put together specific contingency plans to put our services back on track. Where the disaster has damaged a building, we will go through the proper channels with our insurers to identify costs and carry out remedial works.

Industrial Action / Mass Resignations - Catch22 has assessed the risk of mass industrial action / staff walk out as extremely unlikely, especially for key management staff, given our staff turnover and 'open' communication culture which encourages early resolution of any dissatisfactions or staff problems.

We also recognise the importance of holding regular supervision and contribution reviews to sustain employee motivation.

We recognise that any action that affects all employees, such as pay cuts or redundancies, must be carried out with appropriate consultation and recognition of their rights and relevant legislation.

Economic Downturn - Catch22 recognises the risk that an economic downturn poses to the continued successful operation of our business. In the case of such a downturn a structured financial review will be implemented in all our operations and support functions to target cost efficiency savings, identify any potential need for redundancies, and to forecast future cash flow and its effect.

Continuous monitoring of the economic environment in which we operate, and our own financial performance is embedded in regular reporting to senior management and the Trustee Board.

Frequency of Testing - Catch22 recognises that it is important to test our continuity mechanisms so that we can be sure that they will operate effectively in 'real' circumstances. This is owned by a central Gatekeeper, sitting under Director of

Governance, Risk and Compliance, who will ensure the annual testing. This role will also push out updates or changes to the policy.

Disaster recovery testing on our IT systems is also conducted once a year.

We maintain up to date Fire Marshall & First Aid training and records for all of our services and office locations in line with the minimum necessary requirements.

7. Related policies

- Annual and special leave policy
- Flexible working policy
- Health and Safety policy
- Home working policy
- Critical Incident policy
- Property management policy
- Risk Management policy
- Behaviour Management policy
- DP 02 Data and Record Management Policy
- IS09 Information Security Business Continuity Policy
- Mental Health First Aid policy

8.

<TEMPLATE> BUSINESS CONTINUITY MANAGEMENT PLAN

Contents	Page
1. Aim of a BCP and when to invoke this plan	2
2. Service overview	3
3. Approach	3
4. Risk mitigation and local arrangements	4
5. Reporting Required Following Occurrence of Incident	7
6. Contact List of Telephone Numbers	8
7. Checklist of action to be taken	9
8. Testing and reviewing of Business Continuity Plans	10
9. Critical Incident process	10
ANNEX – Guides	13

1) Aim of a BCP and when to invoke this plan

The aim of the **Business Continuity Plan** is to enable Catch22 to continue to deliver an acceptable level of service of its critical activities in the event of any unexpected disruption.

The following scenarios invoke the Business Continuity Plan:

- If the incident impacts:
 - Risk to life, health, safety, or wellbeing of people
 - Significant Financial Impact
 - Business Reputation
 - Legal and / or Regulatory Compliance
 - Disruption, temporarily or longer term, to business-as-usual delivery of services
- If a member of the Chief Officers Group invokes it

A **critical incident** is an event that causes (or has the potential to cause) a severe impact, such as significant disruption to the safety of a staff member or service user, or the delivery of a service. The goal is to ensure safety and minimise damage.

For example (not exhaustive):

- Threat to life, or death of service user, staff member, volunteer, or stakeholder, arising in connection with the work of Catch 22
- Multiple significant injuries from one incident
- Bomb scares or imminent terror attack in the near vicinity
- Fire, flood or explosion
- Extensive damage to premises
- The release of hazardous substances near or on the service site
- IT Systems compromised due to cyber-attack or significant information security breach
- A serious road traffic incident involving a Catch22 vehicle
- Potential media exposure

Critical Incident Plan, or Business Continuity Plan?

If the incident will potentially have a severe impact as described above, please invoke the Critical Incident Plan (part 9). The Hub SLT or Pharos may support to enact the Business Continuity Plans alongside this, to manage disruption to the service once safety is assured.

The principle of '**prudent over-reaction and rapid de-escalation**' applies when making the decision to declare a Critical Incident or Emergency. It is easier and usually more effective to scale down an over-reaction than it is to escalate an under-reaction.

Any other incident which causes disruption to Business-As-Usual practices, please invoke the Business Continuity Plan.

2) Service overview

Name of service:	
Service leader:	
Hub leader:	
Key services provided:	
Key locations:	

3) Approach

This plan details the steps to be taken which are common to all locations to avoid or minimise the likelihood of the occurrence of such an incident and the impact of that incident should it occur (Risk Mitigation and local arrangements – part 4).

It also identifies the steps to be taken to notify the relevant parties which are common to all locations should such an incident occur (Reporting Required Following Occurrence of Incident – part 5).

The plan identifies 3 key roles should an incident occur:

- I. **Responsible Director** - if out of normal business hours, then initially this will be Pharos. Responsibility will normally be transferred as soon as practical to the Director/Hub SLT with responsibility for the location affected. Responsibilities include:
 - Nominating a Local Lead
 - Nominating an Incident Support Manager
 - Providing advice and support to the Local Lead
 - Informing the CEO, Chief Office Group, other Directors, and Trustees as appropriate.
 - Ensuring the Communications and Engagement team are informed if there is a possibility of media interest.
 - Pharos contact number: 0118 380 0540

- II. **Local Lead** (usually the location manager) who will lead, on the ground, with the immediate issues relating to staff, service users, commissioners and continuing to provide local services.

- III. The **Incident Support Manager** (normally but not always the Director of Business Services) whose role is to allow Local Leads to concentrate on local matters.

Responsibilities include:

- Informing insurers, co-ordinating claims, and discussions with loss adjusters
- Support as regards provision of alternate premises, services, and supplies.
- Providing practical help and advice to the Local Lead.

4) Risk Mitigation

This section outlines the existing arrangements which should be in place in all locations to avoid or minimise the likelihood of an incident taking place and to reduce the impact should such an incident occur. It is the responsibility of managers with responsibility for each location to make sure these arrangements are, indeed, in place and, if they are not, to take immediate action to put them in place. Once in place they should be updated and reviewed on at least an annual basis.

STAFF

<i>Are there staff critical to the delivery of the service? If they are not available, can the service open as usual?</i>	
Local arrangement response	
<i>Record out of office contact details for all staff so that contact can readily be made advising them of the situation and arrangements to be made should an incident occur. Identify extent to which they can work from home if necessary. Contact lists should be kept securely off-site and copied into a "Business Continuity" folder within the service's shared drive on SharePoint as necessary. Detail where these are saved and who has physical copies. Can any staff not work from home? Give details of contingency plans if not.</i>	
Local arrangement response	
<i>In the event of an outbreak of a serious disease, or in the event of staff being unavailable or unable to get into work, managers must ensure they have suitable plans for notifying partner agencies, referrals sources, service users, commissioners, other stakeholders, and their staff group of the measures being taken to manage the situation. These measures may include working from a different location e.g. home, reducing contact with other staff and service users (emergencies only), ensuring suitable health and hygiene measures are implemented and used.</i>	
Local arrangement response	
<i>Managers must ensure that they have details of the key contacts they need to access in the event of a health, environmental and/or building incident or emergency e.g. the local public health office, environmental health office, landlord or managing agent including out-of-hours details etc. Who are the key contacts and where is this information saved?</i>	
Local arrangement response	
<i>Are there staff who are first aid trained? And/or mental health first aiders? Where is this list saved, and how are they contacted?</i>	
Local arrangement response	
<i>Please confirm that all staff have the correct next of kin details on People First. This should be reviewed on at least an annual basis.</i>	

Local arrangement response	
----------------------------	--

SERVICE USERS

<i>Record contact details for all service users so that contact can readily be made advising them of the situation and arrangements to be made should an incident occur. Contact lists should be kept securely on-site and copied into a “Business Continuity” folder within the service’s shared folder on SharePoint, as necessary.</i>	
Local arrangement response	
<i>Are there any service users with restrictions in mixing with certain people (or it would be inappropriate to do so). Please consider how this may affect a lockdown scenario.</i>	
Local arrangement response	

CRITICAL SUPPLIERS

<i>If any supplies are crucial to the running of the service/function compile a list of these critical suppliers with contact details so that replacement items can be easily obtained. Contact lists should be kept securely off-site and copied into a “Business Continuity” folder within the service’s shared drive on SharePoint, as necessary. Detail where these are saved. Contact details for critical suppliers should be saved in section 6 below.</i>	
Local arrangement response	

COMMUNICATION SYSTEMS

<i>In the event of a failure of telephony or IT equipment/systems, ensure that the issue is reported and escalated according to the requirements of the system involved. Managers must ensure they have contact details for systems providers and escalation points recorded in an accessible format in the event of their failure. What contingencies are in place for each of the systems should they fail? Contact details for all systems should be saved in section 6 below.</i>	
Local arrangement response	
<i>If access to the Catch22 IT system is due to local telephony or cabling issues, then alternative work areas can be sought. Catch22 systems are designed to be resilient and accessible as long as a suitable internet connection can be established; accessing data on insecure Wi-Fi provision is not permitted. Any failure of the main Catch22 “cloud” service will be managed via the Facilities & IT office. What contingencies are in place for Catch 22 cloud services, including Microsoft and their effect on the service?</i>	
Local arrangement response	

STAKEHOLDERS / COMMISSIONERS / PARTNERS

<p><i>Compile a list of contacts so that stakeholders can be informed of the situation. Contact lists should be kept securely off-site and copied into a “Business Continuity” folder within the service’s shared drive on SharePoint, as necessary. Include any non-critical suppliers not otherwise listed above. Detail where these are saved.</i></p>	
Local arrangement response	

PREMISES (answer for all separate sites)

<p><i>How do we know who is in the building? And can account for all staff, service users, other stakeholders?</i></p>	
Local arrangement response	
<p><i>Is there a minimum service level needed for the site to open safely? What action is taken if this service level isn’t reached?</i></p>	
Local arrangement response	
<p><i>If an incident occurs outside (or inside) the building and a lockdown is required, how is this handled?</i></p>	
Local arrangement response	
<p><i>Ensure all property risk assessments are in place and all recommendations acted on including provision of fire exit notices, fire detection and/or fire suppression systems, appointment and training of fire wardens and regular fire drills and testing of evacuation procedures and equipment. Please provide a hyperlink to where this is recorded.</i></p>	
Local arrangement response	
<p><i>If safe and/or possible, take appropriate action prior to an event to minimise the potential impact, e.g. in the case of a potential flood it may be possible to use sandbags, in the case of severe weather like high winds, it may be possible to board doors and windows etc. Does the site have these available? Where are they stored?</i></p>	
Local arrangement response	
<p><i>If heavy snowfall is predicted, and your service is responsible on site for reducing this risk, take appropriate action to ensure that a plentiful supply of salt/grit and/or snow shovels are available to help clear access routes to the premises if necessary. Where is this stored?</i></p>	
Local arrangement response	

During a terrorist alert/attack, it may be the case that mobile phone signals are suspended for a period of time, and it would be prudent to consider alternative methods for contact in such an event. Public transport links might also be affected/suspended, and consideration should be given to making contingency transport arrangements during such an event.

Local arrangement response

In the event of an incident, can the service be delivered virtually, and how long for? Is there another Catch 22 site nearby that could be used to deliver the service on an alternative temporary basis, following a risk assessment? Are there any stakeholders or external providers associated with the service that may be able to provide temporary premises? [At this point, we do not expect them to be approached, just for consideration].

If a longer-term solution is required, please contact the Director of Workplace & IT.

Local arrangement response

SERVICE DELIVERY

Record contact details for all service users so that contact can readily be made advising them of the situation and arrangements to be made should an incident occur. Contact lists should be kept securely on-site and copied into a “Business Continuity” folder within the service’s shared folder on SharePoint, as necessary.

Local arrangement response

What services are business critical, and should be given priority to restore?

Local arrangement response

5) Reporting Required Following Occurrence of Incident

All incidents must be reported via the Catch22 incident reporting process (Datix).

Incidents regarding data or IT

- If an Information Security incident is identified (including but not limited to any breach/data loss), the Data Protection Officer (DPO), line manager and relevant director and be notified immediately.
- Failure of telephony or IT equipment/systems should be reported and escalated according to the requirements of the system involved.
- If the main Catch 22 ‘cloud’ service fails, contact Director of Workplace and IT.

Incidents regarding people

- The Wellbeing & Safe Practice Team must be alerted.
- In the event of a health (infectious disease) or environmental concern or incident, managers must contact the local responsible officer in public health or the local authority and follow their instructions and advice.

Incidents regarding premises

The steps to be taken following an incident will vary depending on its severity and the services affected. There are however some generic actions that need to be taken in respect of all major incidents. These are detailed below:

- If the situation is local to or specific to one of our buildings, the local manager or staff should ensure the Emergency Services have been called.
- In the event of a major incident, such as a terrorist attack, riot, natural disaster etc., it may be the case that whilst the premises is not damaged, access to the building might be restricted by the police/emergency services. Liaison with the emergency services is essential to ascertain the likely timescales involved until access is granted.
- If the situation calls for it and ***it is safe to do so***, the local manager or staff must, as far as possible, make sure no one is still inside the building or has been injured or killed in any related event.
- The Workplace Team must be alerted.

Incidents regarding reputation

- Contact Director of Communications and Engagement

Outside normal business hours, the local manager or staff must report the incident using the emergency out of hours contact number **0118 380 0540** which is monitored by Pharos and follow the '*Critical Incident Management Process Section 9*'. Pharos will provide immediate support and advice as appropriate.

If for any reason Pharos cannot be contacted staff should use one of the contact numbers for other Directors detailed at the end of this report.

6) Contact List of Telephone Numbers (operational services)

Pharos Out of Hours Support: 0118 380 0540

Details of the line management for each service/location should be completed in the table below and kept up to date. Additional names and numbers can be added as required:

Name	Role	Mobile	Landline
	Strategic Director		
	Director		
	Head of Service/Ops or Assistant Director		
	Head Teacher		
	Service Manager		

There may be circumstances where corporate services directors or assistant directors will also need to be contacted and their contact details are given below: -

Name	Role	Mobile	Landline
Jon Davenport	Director of Workplace & IT	07872422513	01959 578248
Melissa Milner	Director of External Affairs and Partnerships	07734824610	0207 336 4837

Naomi Hulston	Chief Executive Officer	07831711437	020 7336 4800
Christina Duru	Chief People Officer	07778358383	
Nigel Richards	Deputy Chief Executive Officer	07717290559	020 7336 4851
Liz Cole	Head of Wellbeing & Safe Practice	07795428336	01959 578244
Graham Vagg	Head of Safeguarding	07733128738	
Ben Wright	Head of Information Security & Data Protection		01959 578221
Nick Thatcher	Director Governance, Risk & Compliance	07789853896	
Andy Canniford	Chief Development Officer	07795428363	

Services may also need to inform local partners/commissioners/other agencies or suppliers of any serious service interruption. Key contact details for these people/organisations should be completed below and kept updated: -

Name	Organisation	Number	Mobile

7) Checklist of action to be taken

Action	Considered?
Have Emergency Services been called?	
Are all staff and service users accounted for?	
Responsible Director identified? Or Pharos if out of hours?	
Staff notified of Service disruption and next steps / next update?	
Service users notified of Service disruption and next steps?	
Has Local Lead been identified?	
Has Incident Support Manager been identified and informed?	
Have key stakeholders been identified and informed?	
If necessary, are premises secured?	
Has CEO/COG/Trustees been informed?	
Has Communications & Engagement team been informed if possibility of media interest?	
Has Incident been recorded?	
Has Post Incident Review Form been completed?	

8) Testing and Review of Business Continuity Plans

	Date		Date
Last tested		Next test	
Last reviewed		Next review	

9) Critical Incident process

If a critical incident occurs, all staff must consistently apply the following process:

Step 1: Apply SAFE protocols

In the event of a suspected critical incident, it is the responsibility of the local service or school to enact the SAFE protocol. These actions should be taken immediately. Whilst there we cannot place a time limit on t enacting the SAFE protocol, it will typically be expected that escalating and reporting will take place immediately if it is safe to do so and no later than 4 hours of the incident taking place.

- **Safety:** ensure safety of yourself first (ensure you are removed from danger or imminent risk of harm). This step also involves ensuring the safety of service users and or staff.
- **Ask:** ask for assistance from Catch22 managers and colleagues, or Pharos out of hours team if appropriate. Call emergency services if required.
- **Follow:** Catch22 policies and incident reporting procedures to capture information about what has happened and how it occurred.
- **Escalate:** to Hub SLT – Director to be informed if available

The notified Hub SLT member has the responsibility of escalating to the CMIT to triage response on actions to be taken (team will also consider additional measures, such as what help and support other staff / service users may need and what internal investigations need to take place and who will be leading on this). The SAFE protocol ends with triage and actions arising out of the triage call. This should be done by emailing the Critical Incident Team mailbox (criticalincident@catch-22.org.uk) or calling Head Office main number on 020 7336 4800. The CMIT will triage with the Hub Director if this is a Critical Incident and ensure the CLEAR protocol is in place.

Out of Hours

If a critical incident occurs outside of Catch22 core operating hours (9-5). Pharos Response will lead on the response and information gathering and hand over to the Hub Director (or Hub SLT if Director is unavailable) and CMIT at the earliest opportunity, no later than the start of the next working day. Pharos can be contacted on **0118 380 0540**

Step 2: Organisational management of the critical incident will be overseen by the CMIT.

This will be enacted as soon as practically possible and no later than 24 hours from being notified by the Hub Director of the Incident (and or the out of hours team). The CMIT will assemble via a dedicated Teams Channel created specifically for the management of the incident and sharing of information.

The role of the CMIT

It is the responsibility of the Critical Incident Management Team to enact the CLEAR protocol and refer to the Business Continuity Policy and local plan if necessary.

- **Communications** – ensure the communications team are briefed as instructed by Director of Comms. Ensure local service team is briefed and updated on the actions to be taken. Ensure Trustee board is briefed. Consideration should be made if incident should be reported to external regulatory bodies.
- **Learn more** – Relevant investigations may be launched at this point based on information that we have acquired. The incident recording forms will be reviewed using the fishbone method to determine what investigations need to commence.
- **Environment** – consider the setting staff are in and whether changes need to be made to the setting or if more staff resource is required. Ensure the management of any event, additional support will be made available using the resources available through health and wellbeing and EAP.
- **Advice from specialists** – i.e. LADO, Solicitors, Insurance etc
- **Response** – Development of an action plan for the critical incident. This will include short-, medium- and long-term plans. This will be communicated to the local team, with the Hub Director responsible to monitor and review.

The CMIT will request from the Hub SLT the facts around the incident and a COG member with the CMIT will be brought together to manage the event determined by the level of the incident or emergency and will formally confirm the status of the incident.

The CMIT will identify a project team to respond to the critical incident and it will be expected that the project team will be managed by the relevant Hub Director. The project group should report updates to the COG at timely and appropriate junctions defined by either incident progress or COG reporting requests.

The CMIT may delegate to the Incident Controller (the relevant risk lead), full responsibility to manage the initial response to a Critical Incident and Emergency, including decisions around operational priorities and resource allocation. The Incident Controller is then responsible throughout the event. And should report updates to the CMIT at timely and appropriate junctions defined by either incident progress or CMIT reporting requests.

The CMIT shall comprise:

Critical Incident or Emergency Role	Catch22 position
Incident Controller	Relevant Risk Lead
Operations Manager	Relevant Chief Officer (or delegate)
Health and Safety Manager	Head of Wellbeing & Safe Practice (or delegate)
Communications Manager	Director of External Affairs and Partnerships (or delegate)
Systems Manager	Director of Workplace & IT (or delegate)
Administration Support	Executive Assistant to Chief Officers Group
Project Manager	Hub Director (or delegate)
Safeguarding Lead	Head of - Safeguarding (or delegate)
Risk Lead	Health & Safety (Head of Wellbeing & Safe Practice) Safeguarding (Head of Safeguarding)

	Risk Register (Director of Governance, Risk & Compliance) Data (Data Protection Officer) People (Director of Employee Experience) Comms & Media (Director of External Affairs and Partnerships)
--	--

The CMIT or the relevant Incident Controller, will notify the Communications Team, who will take appropriate steps to ensure information is quickly broadcast to staff, and any external stakeholders.

When the Critical Incident and Emergency Management Plan is activated, these staff will be released from their usual roles to take up their Critical Incident or Emergency management roles if this is required.

Appendix A - Guides

The following are considerations and guides when in a business continuity state. There are not mandatory actions or steps but considerations.

Human Resources

Mental health and emotional wellbeing can be impacted during a crisis or significant change. Consider ways to reduce the impact on people. Consider regular, effective, informative communication. Check in with all impacted staff on a regular basis. Staff can receive support from [Mental Health First Aiders](#), [Employee Assistance Programme \(EAP\)](#), or other external organisation's. Consider the use of temporary staff, outsourced staff, and consultants as needed to maintain and recover operations.

Communicate

Consider your current communication channels with employees, customers, suppliers, and the general public. Consider engaging a professional 3rd party communications and PR company. Maintain appropriate, targeted, timely, informed communication with all parties. Maintain a log of the communications and feedback. Consider appointing a single person as a media contact.

Finance

Consider ensuring that employees are not negatively impacted financially and make early arrangements for the continuation of funds. Consider the allocation of a petty cash fund and or the provision of company payment facilities such as a company credit card to those managing the incident. Keep a record of all financial transactions and costs. Put in place arrangements for out-of-pocket expenses including travel and living expenses. Engage with insurers early to understand what requirements they have and what records they will require.

Buildings and Premises

Follow the guidance of the emergency services. When safe to do so keep visual and audio records of the various stages of the incident. Consider a damage assessment and salvage operation. Consider mail redirects. Implement appropriate on-site temporary security appropriate to the situation.

IT

Ensure continuation of information security where practicable. Provide regular communications with the incident management team in a structured and proactive manner to prevent being inundated with calls and request for updates.

Annex 1: Equality Impact Assessment

1. Summary

This EIA is for:	Business Continuity Policy
EIA completed by:	Nick Thatcher, Director of Governance, Risk & Compliance
Date of assessment:	April 2026
Assessment approved by:	n/a

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, fostering 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?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
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?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	No impact although managers must ensure that any alternative working arrangements are assessed to determine if they have a negative impact and are then mitigated.
Gender reassignment (transsexual, transgender, trans) Does this policy impact on people who are transitioning from one gender to another (at any stage)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Marriage and civil partnership Does this policy impact on people who are legally married or in a civil partnership?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

<p>Pregnancy and maternity (in work this is linked to maternity leave, non-work this is for 26 weeks after giving birth)</p> <p>Does this policy impact on people who are pregnant or in their maternity period following the birth of their child?</p>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<p>Race</p> <p>Does this policy impact on people as defined by their race, colour and nationality (including citizenship) ethnic or national origins</p>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<p>Religion and belief</p> <p>Does this policy impact on people who practice a particular religion or none, or who hold particular religious or philosophical belief or none?</p>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<p>Sex</p> <p>Does this policy impact on people because they are male or female?</p>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<p>Sexual orientation</p> <p>Does this policy impact on people who are sexually attracted towards their own sex, the opposite sex or to both sexes?</p>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

3. More information/notes

Please add any links to key documents or websites to evidence or give further detail on any impacts identified.