Business Continuity and Critical Incident Plan

Target Group: All Caregivers	**Version: 11**	**Issue Date: First Issued 28th March 2014**
Approved by: **Leadership Team (25/7/25)**	**Date Last Approved/Reviewed:** **March 2024**	**Effective Date:** **August 2025-July 2026**

Printed copies are for reference only. Please refer to the electronic copy for the latest Version

Contents

1. Introduction

This Business Continuity and Critical Incident Plan sets out the structured response of Holy Cross Hospital to significant disruptions that could impact patient care or core operations. It outlines mitigation strategies, roles, responsibilities, and response actions in alignment with the NHS Emergency Preparedness, Resilience and Response (EPRR) Framework and the Care Quality Commission (CQC) requirements. This plan will be formally reviewed and updated annually or sooner following a major incident, legislative change, or significant operational restructure to ensure it remains current, compliant, and fit for purpose.

2. Purpose

The purpose of this policy is to ensure that Holy Cross Hospital is prepared to respond effectively to any disruption or critical incident that threatens the safety of patients, Caregivers, or the continued delivery of essential services. It provides a structured, consistent approach to identifying risks, initiating timely interventions, and coordinating recovery. This plan promotes operational resilience, minimises service downtime, and supports compliance with regulatory expectations set by the NHS Emergency Preparedness, Resilience and Response (EPRR) Framework and the Care Quality Commission (CQC). It is designed to safeguard life, protect infrastructure, and maintain confidence in the organisation's ability to manage crises safely and efficiently.

3. Objectives of this Policy or Procedure

- Ensure continuity of essential services in the event of a major incident.
- Minimise impact on patient care and wellbeing.
- Provide a clear framework for managing emergencies.
- Define roles and responsibilities of key personnel.
- Maintain regulatory compliance with CQC expectations.

4. Policy Statement

Holy Cross Hospital recognises the critical importance of preparedness in ensuring the safety of patients, Caregivers, and essential services during times of disruption. This Business Continuity and Critical Incident Plan reflects our commitment to proactive risk management, structured incident response, and coordinated recovery. The policy ensures all levels of the organisation—from frontline Caregivers to leadership team—are equipped with clear procedures, defined roles, and tested response tools. It provides a governance framework that supports compliance with CQC standards while fostering a culture of resilience, accountability, and continuous improvement.

5. Scope

This plan applies to all departments, services, Caregivers, contractors, and volunteers operating within Holy Cross Hospital. It covers disruptions due to natural, technical, human-made or external events that compromise critical services.

6. Responsibilities

- **Chief Executive Officer (CEO):** Leads overall coordination of the Business Continuity Plan, liaises with regulators, commissioners (CQC), and external agencies. Responsible for high-level decision-making, strategic oversight, and media relations.
- **Director of Patient Services:** Ensures continuity of safe, effective patient care. Leads the nursing and clinical teams in the prioritisation of clinical services and risk mitigation. Oversees patient safeguarding and infection control measures. Liaises with ICBS.
- **Director of Finance**: Ensures continuity of all financial operations, including payroll, procurement, and contractor payments. Manages budget adjustments during incidents, supports preparation of insurance claims, and oversees the Information Services Manager to ensure continuity of IT infrastructure and information governance
- **HR Manager:** Maintains up-to-date information on Caregivers availability, coordinates deployment and car-sharing initiatives. Responsible for supporting Caregivers wellbeing and overseeing the integration of agency or volunteer personnel into the workforce.
- **Director of Operations:** Oversees critical infrastructure and non-clinical services including facilities, housekeeping, catering, maintenance, and suppliers. Ensures timely access to alternative supply routes and contractor support during incidents.
- **Information Services Manager (ISM):** Leads the recovery and security of digital systems and data. Maintains off-site backups, supports continuity of IT functions, and manages cyber incident response.
- **Nurse-in-Charge (Bleep Holder):** First responder for incident escalation during clinical shifts. Initiates the BCP when necessary, ensures immediate patient safety, and coordinates with emergency services until senior managers assume command. NIC to contact Senior Manager on Call and Maintenance Officer on call if required.

7. Definitions

- **Business Continuity** – The capability of the organisation to maintain essential services during and after a disruption or critical incident.
- **Critical Incident** – Any unexpected event that significantly impacts the hospital's ability to deliver care, protect life, or maintain operational safety, including utility failures, fires, cyberattacks, or extreme weather.
- **Major Disruption** – An event or condition that affects core services or facilities to the extent that immediate intervention or a change in normal operations is required.
- **Essential Services** – Clinical or operational services that are vital to patient care and must be maintained during disruption, such as medication administration, infection control, emergency response, and utilities.
- **Incident Commander** – The person designated to lead the response during a critical incident; usually the CEO or a delegated senior manager.
- **EPRR** – Emergency Preparedness, Resilience and Response: the NHS framework for ensuring organisations can plan for and respond to emergencies.
- **Resilience** – The ability to anticipate, absorb, adapt to, and recover from a disruptive event while continuing to deliver essential functions.
- **Recovery Phase** – The stage following a disruptive incident where services are gradually restored to normal levels, risks are reassessed, and lessons learned are captured.

8. Policy or Procedure Implementation

Plan Activation and Deactivation

The plan is activated upon identification of a threat to business continuity. During normal working hours, the Chief Executive Officer (CEO) or nominated deputy will assess the situation and initiate the BCP if thresholds are met. Outside of normal working hours, the Bleep Holder on-site is responsible for assessing the situation, initiating the BCP if required, and contacting the Senior Manager on Call to escalate the incident and coordinate next steps. Deactivation occurs when normal operations resume and a review has been completed.

Training and Testing

Training ensures that Caregivers are equipped with the knowledge and confidence to respond effectively to a business continuity incident. It is a key component of preparedness and resilience.

- Mandatory annual training is delivered to all managers and designated key response Caregivers.
- Training covers incident identification, BCP activation procedures, communication protocols, and role-specific actions.
- Table top exercises simulate realistic scenarios to assess team readiness and identify improvement areas.
- Live drills (e.g. evacuation or IT outage simulations) are carried out at least once a year.
- Learning from real incidents and exercises is reviewed and incorporated into updated procedures.
- All training activities are recorded in the Training Database

9. Regulatory Requirements/ References

This plan aligns with statutory and regulatory obligations governing emergency preparedness and continuity of healthcare services, including:

- **NHS England Emergency Preparedness, Resilience and Response (EPRR) Framework** – sets the standards for NHS organisations to plan, prepare, and respond to major incidents and business continuity challenges.
- **Care Quality Commission (CQC) Fundamental Standards** – specifically regulations 12 (Safe Care and Treatment), 15 (Premises and Equipment), and 17 (Good Governance), which require providers to ensure safe, well-maintained, and effectively governed services.
- **Health and Social Care Act 2008 (Regulated Activities) Regulations 2014** – outlines provider responsibilities around safety, Staffing and service continuity.
- **Data Protection Act 2018 / UK GDPR** – ensures the protection and proper handling of personal data during and after disruptive events.
- **Equality Act 2010** – requires reasonable adjustments and equitable care provision during incidents affecting normal operations.

10. Evaluation Measures

To ensure the plan remains effective, relevant, and responsive, the following evaluation measures will be applied:

- **Annual Review**: The Business Continuity Plan will be reviewed annually by the Director of Operations, in collaboration with Leadership Team, and updated in response to changes in services, risks, or infrastructure.
- **Post-Incident Review**: After any activation of the plan, a structured debrief will be conducted within 3 working days. Findings will be submitted to the Leadership Team and the Health and Safety Committee.

- **Tabletop Exercises**: At least one annual simulation exercise will be held to test the plan under controlled conditions. Participation and feedback will be documented and used to refine processes.
- **Training Compliance Monitoring**: Training Records will be reviewed quarterly to confirm that all relevant Caregivers have received induction and refresher training.
- **Risk Register Updates**: Lessons learned from exercises and incidents will be reflected in the organisational risk register.

11. Related Documents

This Business Continuity and Critical Incident Plan should be read in conjunction with the following key documents that support risk mitigation, emergency preparedness, and recovery procedures:

- **Major Utility Failure Policy** – Procedures for responding to utility outages and maintaining safe operations.
- **Fire Policy** – Evacuation procedures and fire risk protocols.
- **Managing Extreme Weather Conditions Policy** – Operational planning for heatwaves, snow, flooding, and storms.
- **Infection Prevention Policy** – Continuity arrangements during infectious outbreaks or pandemics.
- **Health and Safety Policy** – Core responsibilities and reporting routes for maintaining a safe working environment.
- **Information Incident Response Plan** – Procedures to responding to cybersecurity incidents, information breaches and failures of IT systems.

12. Appendices

APPENDIX 1 – Equality impact Assessment (EIA) Tool

To be considered and where judged appropriate, completed and attached to any policy document when submitted to the appropriate committee for consideration and approval.

Policy Title	**Business Continuity and Critical Incident Plan**

		Yes/No	**Comments**
	Does the policy/guidance affect one group less or more favourably than another on the basis of:		
	Race	No	
	Gender reassignment	No	
	Marriage & civil partnership	No	
	Pregnancy & maternity	No	
	Ethnic origins (including gypsies and travelers)	No	
	Nationality	No	
	Sex	No	
	Culture	No	
	Religion or belief	No	
	Sexual orientation	No	
	Age	No	
	Disability- both mental and physical impairments	No	
2.	Is there any evidence that some groups are affected differently?	No	
3.	Is the impact of the policy/guidance likely to be negative?	No	
4.	If so can the impact be avoided?	N/A	
5.	What alternatives are there to achieving	N/A	

	the policy/guidance without the impact?		
6. >--	Can we reduce the impact by taking different action?	N/A	
7.	If you have identified potential discrimination, are any exceptions valid, legal and/or justifiable?	No	

Appendix 2. Key Contacts -

- Updated list of all key personnel with mobile numbers, email addresses, and alternative contact methods will be maintained by HRM

IT Support		
cfc	Cyber-insurance provider Policy no: ESL0039564608	0800 975 3034 cyberclaims@cfc.com
Virtual IT	Main IT support (server & network)	020 7644 2820 support@virtualit.cloud
Exchequer	Accounts software support line	03301 224 402
Accounts IQ	New accounts software	support@accountsIQ.com
TM3	Outpatients management system	03333 442 800
AirIT	Cabling infrastructure. Education broadband line (call-barred telephone line: 01428 642344)	0345 565 1953 - Option 1 support@airit.co.uk
ARO	Telephone system support	0330 440 4444 https://bolt.arrowcommunications.co.uk/ Username: reception@holycross.org.uk Password: FreyaChops21*
Reborn Media	Website support	01234 929888 ally@rebornmedia.co.uk

Information Commissioner’s Office	Breach reporting helpline	0303 123 1113
NHS Digital	Cyber security reporting	0300 303 5222

Out of Hours Contractors		
Area of Issue	Contractor who will attend	Contact details and response times
Electrical issues, Plumbing issues	Paine Manwaring	Ring 01903 237522 and select option 1 for plumbing/heating and option 2 for electrical.
Issues with Lifts (NOT including persons trapped)	Elan Lifts	01322 559402 (attendance within 4 hours)
Persons trapped in lift	Elan lifts (	01322 559402 (attendance 90 minutes) also auto dialler from lift car will go over to emergency response number
Fire Alarm Panel/system	Southern Fire Alarms	02392 242016 with 4 hours
Nurse Call system	Aid Call (number is on Panel in Server room)	Can solve majority of issues Remotely 01670 352371
Drains (blockages)	Pipe view	01252 663057
Generator	Ian Webb	Call Out call out no’s are 01296 771000 Mon – Fri 8 – 4.30 outside these hours 07836 729076/ 07876 358222 or 0770370888
Electricity supply issues	British Gas	0845 6005122
Water supply	South East Water (Castle Water)	0333 000 9988/0333 000 0365
Sewage:	South East Water	0333 000 9988 /0333 000 0365
Gas Pipework (OUTSIDE THE BUILDING)	Transco	0800 111 999

Gas	Leak alert	0333 000 0365
Gas Supply	British Gas	0845 6005122
Generator Fuel		Certas Energy UK Limited Westerleigh Terminal Oakley Green Westerleigh - Bristol - BS37 8QE OR Nationwide Fuels 0845 0303111
Computer Network issues	Virtual IT	0207 644 2820
Catering equipment	Tyrells	01483 776684
Refrigeration Equipment	RS Refrigeration	01256 760 633

Appendix 3 Emergency Checklists

1. Staffing emergency checklist (minimum cover, contact procedures, car share planning)
2. Infrastructure failure checklist (evacuation steps, damage logging, relocation zones)
3. Financial Services Disruption Checklist
4. Utility failure checklist (backup equipment, key shut-off points, fuel checks).
5. Supplier failure checklist (stock levels, alternative supplier list).
6. IT failure checklist (manual procedures, data recovery protocols).
7. Bomb threat checklist (communication tree, control room readiness).

1. **Staffing Emergency Checklist** Facilitated by: HR Manager/DPS

This checklist supports the continuity of care during Caregivers shortages due to illness, adverse weather, transport disruption, or infectious outbreaks. It should be activated immediately when Staffing levels fall below safe thresholds for any department.

Immediate Actions:

- Identify departments below minimum safe Staffing levels using the centralised rota and absence reporting system.
- Contact all available Caregivers via phone, Whatsapp, SMS, and email using the central Caregivers contact log.
- Confirm which Caregivers can report for duty and expected arrival times.

Redeployment and Support:

- Redeploy available internal Caregivers to highest priority areas (e.g., Wards, meal preparation, and medication administration).
- Notify department heads of redeployment needs.

- Contact pre-approved bank Caregivers, volunteers, and agency personnel for short-term cover.
- Assess the skill mix of remaining Caregivers and allocate duties based on competency.

Accommodation and Travel Support:

- Liaise with Facilities & Housekeeping Lead to prepare on-site Caregivers accommodation rooms.
- Implement car-sharing plans for Caregivers in neighbouring areas, ensuring GDPR-compliant sharing of limited contact details for coordination.
- Monitor local travel and weather reports to plan shift transitions and risk areas.

Communication and Coordination:

- Provide Caregivers and managers with regular situation updates.
- Work with the Nurse-in-Charge and Director of Operations to assess critical risk to services.
- Escalate concerns about Staffing to the CEO or Director of Patient Services immediately if patient care is at risk.

Sustaining Operations:

- Implement a reduced or prioritised service model, suspending non-essential services (e.g., outpatient appointments, meetings).
- Use split-shift or staggered shift models to maximise coverage.
- Monitor Caregivers wellbeing and ensure sufficient breaks and rest periods are maintained.

Documentation:

- Record all Caregivers redeployments, absences, and rota adjustments.
- Log communications and decisions taken.
- Document any critical incidents related to Staffing and submit for review post-incident.

Recovery:

- Continue daily review of Caregivers availability.
- Revert to normal operations once staffing levels are stabilised and services have been fully restored.

2. Infrastructure Failure Checklist Compiled by: Director of Operations

This checklist provides structured actions for responding to infrastructure failure events, including fire, flood, structural collapse, and other physical damage to the hospital estate. The goal is to protect life, maintain safety, secure assets, and restore operational capability.

Immediate Actions:

- Activate the emergency alarm system or fire evacuation protocol depending on the nature of the event.
- Call emergency services (999) if required.

- Confirm evacuation of all patients, visitors, and Caregivers from affected zones using known exits.
- Direct relocation to pre-identified temporary zones: gyms, chapel, lounges, or patients activities
- Nurse-in-Charge to complete roll-call and confirm headcount with Senior Manager on duty.

Damage Assessment and Containment:

- Do not enter compromised areas until declared safe by emergency services or caretaking team.
- Assign Maintenance Officer to assess extent of damage and utility disruption.
- Take photos and notes for insurance purposes.
- Shut off utilities in the affected area (e.g., power, gas, water) if safe to do so.
- Use temporary barriers, signage, or tape to prevent access to hazardous zones.

Communication and Reporting:

- Notify CEO and Director of Operations with a situational summary.
- Inform external stakeholders including the ICB, CQC, and insurers.
- Deploy media holding statement if disruption is prolonged or visible to the public.

Continuity of Services:

- Assess which essential patient services can continue safely in unaffected zones.
- Coordinate with Director of Patent Services and Director of Therapy to determine safe operational areas.
- Suspend non-essential services and reassign Caregivers accordingly.
- Source temporary infrastructure support (e.g. mobile welfare units, temporary power supplies).

Recovery and Repair:

- Commission contractor support for inspection and remedial repairs.
- Ensure water ingress is mitigated and environmental decontamination arranged if needed.
- Maintain a repair log and asset damage list for insurers.
- Report back to Leadership Team with timescale for full service resumption.

Documentation:

- Complete Incident Log including: cause, time of event, actions taken, and services affected.
- Submit post-incident review to Leadership Team and Health and Safety Committee.
- Update fire or facilities risk assessments accordingly.

3. Financial Services Disruption Checklist *Facilitated by: Director of Finance*

This checklist outlines response actions in the event of financial system failure, including disruption to payroll processing, supplier payments, and banking access. It ensures continuity of critical financial functions during technical failures, cyber incidents, or third-party service disruptions.

Immediate Actions:

- Confirm the nature and scope of the disruption (e.g., payroll, accounting software, bank access and raising invoices).
- Notify:
    - CEO
    - Information Services Manager/IT support
    - HR Manager (if payroll is affected)
- Contact relevant financial service providers (banks, payroll vendors, ICB, IT support, and other software, Trade shift).
- Activate paper-based or offline contingency finance processes.

Payroll Continuity:

- Confirm next payroll due date and payment risk.
- Notify payroll bureaux to use last month's data to process
- Prioritise staff groups for urgent payment if required (e.g. bank or agency).
- Explore alternative payment methods (manual bank transfers, advances).
- Keep staff updated on status and expected resolution.

Supplier Payments:

- Identify critical suppliers at risk due to payment delays.
- Notify affected departments of potential procurement impacts.
- Discuss temporary credit terms or workarounds with key suppliers.
- Maintain records of verbal agreements and payment commitments.

Recovery and Restoration:

- Coordinate with IT Support to restore financial platforms.
- Identify if appropriate for remote working as new systems are cloud based.
- Monitor integrity of restored data and access rights.
- Document the timeline and outcome of system recovery.

Communication and Documentation:

- Issue internal updates to relevant managers.
- Maintain logs of all communications, actions, and decisions.
- Escalate unresolved risks to the Leadership Team.
- Submit a financial disruption report to the Leadership Team.

Post-Incident Actions:

- Conduct a formal review and root cause analysis.
- Capture lessons learned and update the Finance Contingency Checklist.
- Reflect risks in the Finance section of the organisational risk register.

4. Utility Failure Checklist Compiled by: Director of Operations

This checklist provides comprehensive guidance in the event of failure of gas, electricity, water, telephone or sewage systems. It aligns with the Major Utilities Failure Policy and should be activated immediately upon confirmation of service disruption.

Immediate Actions:

Confirm which utility has failed and identify the specific areas affected.

Notify CEO, Nurse-in-Charge (Bleep Holder), ward leads, and housekeeping & catering teams.

Contact the utility provider to determine the cause, scale, and estimated duration of the outage

Ensure the on-call Maintenance Officer is notified and deployed to assess risks and initiate response.

Electricity Failure:

Emergency generator will automatically activate, carry out regular checks of generator to ensure fuel levels are monitored (48-hour fuel supply available; on-board tank provides 8 hours at 100% load).

Confirm availability of UPS backups for nurse call panels, ventilators, BMS, and telecoms (3-hour capacity).

Ensure all essential systems are transferred to generator power.

Monitor fuel levels and contact Certas Energy or Nationwide Fuels for top-up as needed.

Deploy emergency lighting in designated corridors and wards.

Inform Virtual IT to monitor backup server and initiate data replication.

Gas Failure:

Acknowledge that gas supply has no on-site replacement.

Conserve heat by closing windows and internal doors.

Supply patients with additional blankets (from ward clean store and nurses' residence).

Liaise with the plumbing contractor for provision of portable electric heaters and confirm safe electrical capacity.

Consider sourcing additional standalone generators if additional heating is required.

Adjust catering: use electric hotplates, microwave ovens, and gas barbeque as needed. Domestic-sized electric oven available in the patient activities kitchen.

Water Failure:

South East Water will provide bottled water as the hospital is a priority site.

Use internal storage tanks (up to 48 hours' supply if failure is detected early)- Note this water is not suitable for use as drinking water unless boiled.

Restrict non-essential use (e.g. bathing, flushing).

Boil stored water before drinking.

Purchase bottled water if emergency supply is not sufficient.

Telecoms Failure:

Divert incoming calls to 07818 789183 (held at reception, labelled "INCOMING CALLS").

Outgoing calls to be made via 07563 651405 (hospital mobile used by clinical Caregivers).

Use additional handset held in reception if required.

Report issue using Arrow Communications portal.

Reception to ensure mobile phones are charged and have active credit/contracts.

Sewage/Drainage Issues:

Contact South East Water or Pipe View for emergency attendance.

Prevent usage of affected facilities until issue is resolved.

Coordination & Documentation:

Maintain communication with affected teams and provide regular updates.

Keep a log of actions taken, provider updates, and changes in service impact.

Liaise with external contractors and support services

Recovery:

Confirm restoration of utility with provider and conduct safety checks before resuming normal usage.

Reset systems connected to BMS or telecoms.

Conduct debrief and post-incident review.

Update Leadership Team and submit utility outage report for record keeping.

5. Supplier Failure Checklist Compiled by: Director of Operations

This checklist supports rapid response to any disruption in the supply of critical items such as medication, oxygen, enteral feeds, fuel, catering goods, and clinical consumables. It is informed by the Essential Supplies Risk Assessment.

essential supplies
RA 2025.xlsx

Immediate Actions:

- Identify which supply has failed and which departments are affected.
- Review stock levels in clinical, catering, and maintenance stores.
- Communicate with the department leads to prioritise essential items.
- Initiate contingency supply measures based on risk rating.

Priority Supply Categories:

- **Medication (e.g. Ashtons):** check if alternative stock can be sourced locally. Seek advice from medical professionals. Where appropriate, switch to alternative medications.
- **Enteral Feeds (Nutricia/AAH):** alternative suppliers such as **Abbott and Fresubin** Seek advice from dietitian. Where appropriate, switch to alternative enteral feeds.
- **Oxygen (BOC):** two local depots available.
- **Diesel (Certas Fuels):** 96 hours on-site; contact Certas or Nationwide Fuels if short.

Contact Alternative Suppliers:

- Refer to Appendix A for supplier contact list.
- Liaise directly with AAH, Nutricia, local pharmacy, and others as relevant.
- Confirm estimated time for delivery and emergency options.

Stock Management:

- Implement restricted usage protocols for high-risk items.
- Document current stock levels and expected run-out times.
- Distribute stock appropriately across wards and services.

Communication:

- Notify CEO, Director of Patient Services and Nurse-in-Charge (Bleep Holder).
- Keep ward leads informed of availability and changes in supply chain.
- Record all supplier communications and resolutions.

Documentation and Reporting:

- Maintain logs of all actions taken, including supplier contact, delivery confirmations, and decisions made.
- Submit supply chain disruption report to Leadership Team.

Recovery:

- Confirm restored delivery from primary supplier.
- Review lessons learned and update supplier contingency plans.
- Reflect changes in the Essential Supplies Risk Register.

6. IT Failure Checklist Compiled by: Information Services Manager

This checklist is activated in the event of IT system disruptions, data loss, or cyber incidents affecting the hospital's operations. For detailed information refer to the Information Incident Response Plan (June 2025) and Information Governance Policy.

Immediate Actions:

- Identify the nature of the failure: e.g., hardware, software, network, telephony, or potential cyber incident.
- Notify CEO, Director of Operations, Director of Finance, and Virtual IT support.
- Escalate to Director of Finance if data security is potentially compromised.

Initial Containment:

- Disconnect affected devices from the network if a cyberattack is suspected.
- Activate backup communication methods (hospital mobiles, radios).
- Restrict access to critical systems to prevent further risk.

Manual Operations:

- Revert to paper-based systems for handovers, care notes, medication records, referrals, and admissions.
- Distribute pre-printed templates stored in the nursing admin office.
- Notify all departments of change in process.

Data Protection and Incident Reporting:

- If personal data is affected, assess whether the breach meets the threshold for reporting to the ICO.
- Complete an internal Information Incident Report.
- Maintain audit trail of all access and decisions taken.

Recovery and Restoration:

- Initiate restoration from off-site backups/cloud as per recovery priority order.
- Prioritise clinical systems, Caregivers rota platforms, email, and finance systems.
- Monitor restoration progress and validate integrity of restored data.
- Confirm return of access permissions and user accounts.

Communication:

- Provide regular updates to managers and department leads.
- Use Caregivers noticeboards, mobile alerts, and verbal handovers where email is unavailable.

Documentation:

- Log incident in full: including root cause (once known), detection method, duration of outage, systems affected.
- Document actions taken at each phase.
- Submit review report to Leadership Team.

Post-Incident Review:

- Convene debrief with IT support, operational managers, and leads.
- Update risk registers and cybersecurity procedures if required.
- Capture lessons learned and update the IT Recovery Plan.

7. Bomb Threat Checklist

- Remain calm and do not interrupt the caller if the threat is made by phone.
- Try to obtain as much information as possible (see below for suggested questions).
- Notify the Nurse-in-Charge (Bleep Holder) immediately.

- Contact emergency services (999) and follow their instructions.
- Initiate lockdown or evacuation as directed by emergency services.
- Secure the control room (Reception Office) for coordination.
- Ensure ward Caregivers remain with patients unless evacuation is required.
- Keep thorough written notes of the call or report.
- Inform CEO or on-call senior manager for media and stakeholder response.

Questions to ask if caller makes a threat:

1. When is the bomb going to explode?
2. Where is it right now?
3. What does it look like?
4. What kind of bomb is it?
5. What will cause it to explode?
6. Did you place the bomb? Why?
7. What is your name and address?
8. What is your telephone number?

Observe the caller's:

- Voice (accent, tone, speech patterns)
- Background noise (machinery, traffic, music, voices)
- Any identifiable caller ID information

Post-Threat Actions:

- Complete a Bomb Threat Record Form.
- Debrief with emergency services and leadership.
- Support Caregivers and patient wellbeing.
- Conduct a post-incident review to capture lessons learned.

Appendix 4 Communication Templates

- Incident notification to Caregivers (email/text/WhatsApp example).
- External stakeholder communication (commissioners, CQC, press).
- Media Holding Statement (if required)

Incident Notification Template (Internal)

To: [All Caregivers / Department Name] from: [CEO / Senior Manager / Nurse-in-Charge] Subject: [Incident Name – e.g. IT Outage, Power Failure]

Dear Team,

Please be advised that as of [time/date], we are experiencing [brief description of the incident, e.g., a total IT outage affecting all departments].

Key actions required:

- [e.g. All Caregivers to revert to paper documentation.]
- [e.g. Use emergency phone lines for internal communication.]

Further updates will be provided as the situation develops. Please speak with your line manager if you have immediate concerns.

Thank you for your cooperation.

External Notification Template (Commissioners / CQC / Suppliers) To: [Recipient Name / Organisation] From: [CEO / Director of Operations] Subject: Notification of Business Continuity Incident at Holy Cross Hospital

Dear [Name],

We are writing to inform you that a Business Continuity Incident has occurred at Holy Cross Hospital as of [time/date]. The nature of the incident is as follows:

[Brief overview of the situation and services affected.]

We have activated our Business Continuity Plan and are taking all necessary steps to mitigate disruption and ensure patient safety.

We will provide further updates at regular intervals or as soon as the situation changes. Should you need to contact us directly, please use the following contact:

[Name, Role, Contact Details]

Thank you for your support and understanding.

Kind regards,

[Name]
[Job Title]
Holy Cross Hospital

Media Holding Statement (if required)

"Holy Cross Hospital is currently managing a temporary disruption to its services due to [brief cause – e.g. an IT issue / weather event]. We have activated our Business Continuity Plan to ensure the ongoing safety and care of our patients. Our teams are working closely with partners and suppliers to resolve the issue swiftly. Further updates will be provided as appropriate."

For press enquiries, please contact [CEO Name / Communications Lead, contact number].

Appendix 5 Training Programme

Caregivers Training Programme for Business Continuity and Critical Incident Response

Training Overview: To embed resilience across the organisation, the following training modules will be delivered to ensure Caregivers understand their roles and are equipped to act during disruptions.

1. Induction Session (All Caregivers – within 4 weeks of start date) Content:

- Introduction to the Business Continuity Plan
- Overview of emergency types (fire, flood, IT failure, etc.)
- What to do in the event of a critical incident
- Where to find emergency contact numbers and checklists

Facilitated by Learning and Development **Delivered by:** Director of Operations

2. Role-Specific Workshops (Annually) Targeted to: Nurse-in-Charge, Facilities Caregivers, Reception, IT, Department Leads
Content:

- Incident checklists and lead responsibilities
- Communications and escalation procedures
- Manual workarounds for IT failure
- Relocation and evacuation protocols

Delivered by: Director of Operations or Information Services Manager

3. Desk based Scenario Workshop (Annually): Senior Managers, Information Services Manager, Bleep Holders.
Content:

- Simulated infrastructure, utility, or cyber disruption
- Live walkthrough of the plan under timed conditions
- Identification of gaps, improvements, and debrief

4. Refresher E-Learning (Every 2 Years) Content:

- Short online modules reviewing key principles
- Updates on policy or contact information
- Brief quiz or knowledge check

Delivered by: Learning and Development via intranet

5. Debrief-Led Training (Post-Incident): Caregivers involved in an actual incident
Content:

- Review of actions taken
- Lessons learned and good practice

- Updates to the plan based on real-world outcomes
  Delivered by: Leadership Team, Bleep Holders, Information Services Manager *Depending on incident

Appendix 6. Lessons Learned from respiratory infectious diseases, including COVID-19, Flu and others.

The COVID-19 pandemic exposed and tested the resilience of health and care systems globally. Holy Cross Hospital identified key lessons and has embedded them into this Business Continuity and Critical Incident Plan:

- **Flexible Staffing Models:** The need for agile redeployment of Caregivers, cross-skilling, and resilience rotas has informed the staffing emergency checklist and associated training modules.
- **Stockpiling and Supplier Contingencies:** Supply chain disruption led to the introduction of critical stock monitoring and alternative supplier frameworks.
- **Enhanced Infection Prevention:** Isolation protocols, PPE logistics, and outbreak containment measures are now embedded in the Pandemic Response Policy (Infection Prevention Protocols)
- **Digital Capacity and Remote Working:** Expansion of secure remote access and digital communication has enhanced IT continuity planning.
- **Caregivers Wellbeing and Psychological Support:** Proactive mental health support, resilience training, and reflective supervision are recognised as essential in long-term incident response.
- **Clearer Communication Channels:** Frequent, honest communication with Caregivers, patients, and families was critical and has shaped internal and external communication templates.
- **Decision-Making under Pressure:** COVID-19 emphasised the importance of structured command frameworks, delegated authority, and rapid policy review mechanisms.