

TRUST-WIDE NON-CLINICAL DOCUMENT

BOMB THREAT / SUSPICIOUS PACKAGE PROCEDURE

Policy Number:	SD45-b
Scope of this Document:	Trust wide
Recommending Committee:	Health & Safety Committee
Approving Committee:	Executive Committee
Date Ratified:	March 2019
Next Review Date (by):	January 2021
Version Number:	Version 2
Lead Executive Director:	Executive Director of Communications and Corporate Governance
Lead Author(s):	Head of Health Safety Fire and Security

TRUST-WIDE NON-CLINICAL DOCUMENT

2019 – Version 2

Striving for perfect care for the people we serve

TRUST-WIDE NON-CLINICAL DOCUMENT

BOMB THREAT / SUSPICIOUS PACKAGE PROCEDURE

Further information about this document:

Document name	BOMB THREAT / SUSPICIOUS PACKAGE PROCEDURE (sd45b)
Document summary	This document describes the actions to be taken in the event of a bomb threat or suspicious package being reported on or in the vicinity of Trust premises.
Author(s) Contact(s) for further information about this document	Carlton Brooks Head of Health Safety Fire and Security Telephone: 0151 472 4071 Email: carlton.brooks@merseycare.nhs.uk
Published by Copies of this document are available from the Author(s) and via the trust's website	Mersey Care NHS Foundation Trust V7 Building Kings Business Park Prescot Merseyside L34 1PJ Trust's Website www.merseycare.nhs.uk
To be read in conjunction with	SD45 Lockdown SA31 Major Incident Plan
This document can be made available in a range of alternative formats including various languages, large print and braille etc	
Copyright © Mersey Care NHS Trust, 2015. All Rights Reserved	

Version Control:

		Version History:
Version 1	Policy Group Executive Committee	January 2017 March 2017
Version 2	Update Executive Director	February 2019

SUPPORTING STATEMENTS

this document should be read in conjunction with the following statements:

SAFEGUARDING IS EVERYBODY'S BUSINESS

All Mersey Care NHS Foundation Trust employees have a statutory duty to safeguard and promote the welfare of children and adults, including:

- being alert to the possibility of child / adult abuse and neglect through their observation of abuse, or by professional judgement made as a result of information gathered about the child / adult;
 - knowing how to deal with a disclosure or allegation of child/adult abuse;
 - undertaking training as appropriate for their role and keeping themselves updated;
 - being aware of and following the local policies and procedures they need to follow if they have a child / adult concern;
 - ensuring appropriate advice and support is accessed either from managers, *Safeguarding Ambassadors* or the trust's safeguarding team;
 - participating in multi-agency working to safeguard the child or adult (if appropriate to your role);
 - ensuring contemporaneous records are kept at all times and record keeping is in strict adherence to Mersey Care NHS Foundation Trust policy and procedures and professional guidelines. Roles, responsibilities and accountabilities, will differ depending on the post you hold within the organisation;
- ensuring that all staff and their managers discuss and record any safeguarding issues that arise at each supervision session

EQUALITY AND HUMAN RIGHTS

Mersey Care NHS Foundation Trust recognises that some sections of society experience prejudice and discrimination. The Equality Act 2010 specifically recognises the *protected characteristics* of age, disability, gender, race, religion or belief, sexual orientation and transgender. The Equality Act also requires regard to socio-economic factors including pregnancy /maternity and marriage/civil partnership.

The trust is committed to equality of opportunity and anti-discriminatory practice both in the provision of services and in our role as a major employer. The trust believes that all people have the right to be treated with dignity and respect and is committed to the elimination of unfair and unlawful discriminatory practices.

Mersey Care NHS Foundation Trust also is aware of its legal duties under the Human Rights Act 1998. Section 6 of the Human Rights Act requires all public authorities to uphold and promote Human Rights in everything they do. It is unlawful for a public authority to perform any act which contravenes the Human Rights Act.

Mersey Care NHS Foundation Trust is committed to carrying out its functions and service delivery in line the with a Human Rights based approach and the FREDA principles of **F**airness, **R**espect, **E**quality **D**ignity, and **A**utonomy

Contents

Section	Page No
1. Purpose and Rationale	5
2. Outcome Focused Aims and Objectives	5
3. Scope	5
4. Definitions	5
5. Duties	6
6. Process	7
7. Consultation	17
8. Training and Support	18
9. Monitoring	18
10. Equality and Human Rights Analysis	19
11. Appendix A Action Cards	22
Action Card 1: Action to be taken on receipt of a Telephone Bomb Threat	22
Action Card 2: Actions to be taken on receipt of a Bomb Threat by Email or Social Media	24
Action Card 3: Immediate Actions on Suspicion of Explosive Device/Bomb Threat	25
12. Appendix B Building Evacuation Profile Template	26

1. PURPOSE AND RATIONALE

- 1.1 The purpose of this protocol is to advise and support staff of the Trust on bomb threats and to seek their support and commitment to the creation of an engendered pro-security culture.
- 1.2 This document contains information on the structure required and defines the roles and responsibilities to implement the bomb threat policy.
- 1.3 Security management in simple terms may be defined as a robust, risk measured system for protecting people and property.

2. OUTCOME FOCUSED AIMS AND OBJECTIVES

- 2.1 To integrate security into the general working environment of the Trust and to reduce the risk of a bomb attack.
- 2.2 To support the personal safety, at all times, of patients, staff and visitors.
- 2.3 To protect the Trust's buildings from malicious acts, criminal damage and criminal trespass.
- 2.4 To protect the Trust's assets and information from theft, damage or fraud.
- 2.5 The security of drugs, prescription forms and hazardous material.
- 2.6 The security of maternity and paediatric units.
- 2.7 To protect personal property belonging to patients, clients, staff and visitors whilst on the Trust's premises.
- 2.8 To support the uninterrupted delivery of health and community care.

3. SCOPE

- 3.1 This policy applies to 'all staff' who have a responsibility to ensure that security measures and procedures are observed at all times. Managers should take a lead role in promoting and developing a security conscious environment.
- 3.2 High Secure Services and the secure mailroom at the Maghull site have local policies regarding suspect packages and bomb threat.

4. DEFINITIONS (Glossary of Terms)

Glossary of Terms	Definition
IED	Improvised Explosive Device- devices placed or fabricated in an improvised manner
Bomb Threat	A threat to detonate an explosive or incendiary device to cause property

	Community and Mental Health Services damage or injuries, whether or not such a device actually exists. Bomb threats are usually made over the phone
Suspicious Package	A package believed to contain a potentially harmful device or substance
CBRN	Chemical, Biological, Radioactive, Nuclear
PEEPS	Personal Emergency Evacuation Plans
Incendiary Device	A device designed to cause a fire

5. DUTIES

- 5.1 **Chief Executive** has overall responsibility for controlling and co-coordinating security. However, responsibility for management and implementation of this policy is delegated to the Security Management Director (SMD) and the appointed LSMS. This is in accordance with the Secretary of State Directions of November 2004 and the Security Incident Response plan.
- 5.2 **Executive Director of Communications and Corporate Governance (NHS Protect Security Management Director)**, In line with the Secretary of State Directions is the nominated Trust Security Management Director (SMD). The role of the SMD includes:
- (a) Promoting Security at Board level
 - (b) Agreeing the LSMS work plan and monitoring the delivery of the work plan
 - (c) Ensuring compliance with the requirements and directions issued by the Secretary of State, DH and NHS Protect.
- 5.3 **Chief Operating Officers** are responsible for:
- (a) Ensuring that their division has procedures to manage bomb threats and suspicious packages at each site and that they are fit for purpose;
 - (b) Allocating planning tasks within their respective division.
- 5.4 **Communication and Engagement Team** will
- (a) Help to ensure that a controlled message is broadcasted to staff, patients and visitors within the Trust and to external stakeholders, informing them of the current situation;
 - (b) Developing pre-prepared communication messages for media and external stakeholders.
- 5.5 **Head of Risk and EPRR** is responsible for:
- (a) Ensuring that the Major Incident and Business Continuity Plans and supporting arrangements are cognizant of the Trust bomb threat/suspicious package procedure.
 - (b) Providing advice and support where appropriate.
- 5.6 **Local Security Management Specialist (LSMS)** is responsible for:
- (a) Overall delivery and implementation of this Strategy
 - (b) Ensuring that the SMD is fully aware of security issues which may affect the Trust, its staff, patients or the level of service for which it offers
 - (c) Assisting the Trust to realise the requirements and directions issued by the Secretary of State, DH and NHS Protect relating to security

(d) Producing an annual security report and work plan

5.7 **Police Liaison**

The Trust directly employs x 4 police liaison officers who support the Trust in crime prevention at Ashworth Hospital, Scott Clinic, Rathbone Low Secure Unit, Broadoak and Clock View. The police liaison can provide a local link with Merseyside police and assist in the safe evacuation of the building.

5.8 **Building/Site Manager(s)** will assist in disseminating the policy at local sites and take part in table-top exercises and simulations in conjunction with the local LSMS.

5.9 **Switchboard**, will receive telephone calls reporting bomb threats, call police and escalate to Silver/Gold on call to initiate an evacuation of the building/area.

Complete an incident form (Appendix 'A'; Action Card 1) as per policy.

5.10 **Fire Marshalls/Wardens**, will

- (a) Provide a sweep of the building to ensure everyone is safely evacuated.
- (b) Assist in the implementation of PEEPS.
- (c) Report to the person in charge that the building is clear and place 'Do not enter signs' on exit doors.

5.11 **Gatekeepers**, Senior manager in charge may nominate staff to assist in sweeping the building to:

- (a) Ensure safe evacuation and; or
- (b) Locate and report a suspicious package (NB: suspicious packages should not be touched).

5.12 **All Trust Staff:** have a legal obligation to co-operate and adhere to this policy with regard to its aims. Great emphasis is placed on the importance of the co-operation of all staff in observing security and combating crime and ensuring their own and colleagues' safety in accordance with the Trust's Health and Safety Policy. Every member of staff has a responsibility to familiarise themselves with:

- (a) Any special security requirements relating to their place of work or work practices
- (b) The action to take in the event of a security incident
- (c) To safeguard themselves, colleagues, visitors, patients so far as is reasonably practicable and ensure that neither equipment nor property are put in jeopardy by their actions, either by instruction, example or behaviour
- (d) To follow agreed working methods and security procedures at all times
- (e) To comply with all training requirements concerning security issues
- (f) report any suspicious packages including telephone threats via the command structure/management structure and complete an incident form;

6. PROCESS

6.1 **Notification of a Bomb Threat**, notification of a bomb threat can be made at any time and can be made and delivered by several means, usually anonymous, but all must be considered seriously.

6.2 Telephone Calls

6.2.1 With direct dialing anyone can be on the receiving end of a bomb threat. In such circumstances staff should be mindful of the actions to be taken to help them deal with such a call. A list of actions is contained in the checklist in the Bomb Alert Procedure (See Appendix A, Action Card 1).

6.2.2 These actions include:

- (a) let the caller finish the message without interruption. Try to keep the caller on the line as long as possible and ask where the bomb is located, when the bomb is going to explode, what kind of bomb it is and what it looks like, who placed the bomb and why?;
- (b) ask for the name of the caller and where they are calling from and whether they intend to call back;
- (c) when the caller rings off, dial 1471 (if that facility operates and you have no automatic number display) to see if you can get their number;
- (d) make a note of the callers voice, accent, tone, foul language, etc. and listen for background noise;
- (e) the Police should be contacted immediately whenever a bomb threat is received and should be via the 999 system;
- (f) Silver on Call is to be informed as soon as practicable (NB: Contact Gold on Call where the incident relates to corporate services e.g. V7). The decision to contact communications will be made through the command structure;
- (g) an electronic incident report should also be completed as soon as possible after the incident/stand down. The incident form should contain the full details of incident and where the police have been involved: the police officer's details and the police incident log reference number;
- (h) the advice of the LSMS or Police Liaison (where available) is needed regarding the protection and preservation of the scene of a crime and the (forensic) evidence. The LSMS will carry out a review: of the incident itself, the available evidence, the outcomes and what redress the Trust can pursue in order to ensure this policy is effective.

6.3 Monitoring Post Received

6.3.1 Most mail is received direct from the courier therefore the contents cannot be assured unless the mail is received and signed for from a known source.

6.3.2 The High Secure post room has a local policy for dealing with suspect packages and has the facility to X-ray packages received. X-ray of packages normally only occurs for post intended for the High Secure site.

6.4 Letter Bombs

6.4.1 Letter bombs, which include parcels, packages and anything delivered by post or courier, have been a commonly used terrorist device. It is essential that all sources of incoming mail (e.g. Royal Mail, couriers and hand delivery) are included in the Trust's screenings process.

- 6.4.2 Letter bombs may be explosive or incendiary (the two most likely types) or conceivably chemical, biological or radiological (CBR). Anyone receiving a suspicious delivery is unlikely to know which type it is, so procedures should cater for every eventuality.
- 6.4.3 A letter bomb will probably have received fairly rough handling in the post and so is unlikely to detonate through being moved, but any attempt at opening it may set it off. Unless delivered by a courier, it is unlikely to contain a timing device.
- 6.4.4 Letter bombs come in a variety of shapes and sizes: a well-made one will look innocuous but there may be telltale signs (see 6.5 below).
- 6.4.5 Good housekeeping is essential for safeguarding staff. Ensuring that parcels, boxes and other similar objects are stowed away safely and as soon as possible is a good crime/bomb threat prevention practice.

6.5 Indicators of a Letter Bomb

- (a) it is unexpected or of unusual origin or from an unfamiliar sender;
- (b) there is no return address or the address cannot be verified;
- (c) it is poorly or inaccurately addressed, e.g. incorrect title, spelt wrong, titled but no name or addressed to an individual no longer with the Trust;
- (d) the address has been printed unevenly or in an unusual way;
- (e) the writing is in an unfamiliar style;
- (f) there are unusual postmarks or postage paid marks;
- (g) a jiffy bag or similar padded envelope has been used;
- (h) it seems unusually heavy for its size. Most letters weigh up to about 30 grams, whereas most effective letter bombs weigh 50-100 grams and are 5mm or more thick;
- (i) it has more than the appropriate value of stamps for its size and weight;
- (j) it is marked 'personal' or 'confidential';
- (k) it is oddly shaped or lopsided;
- (l) the envelope flap is stuck down completely (a normal letter usually has an un-gummed gap of 35mm at the corners);
- (m) there is a pin-sized hole in the envelope or package wrapping;
- (n) there is an unusual smell, including but not restricted to, almonds, ammonia or marzipan;
- (o) it has greasy or oily stains on the envelope;

- (p) there is an additional inner envelope and it is tightly taped or tied (however, in some organisations sensitive material is sent in double envelopes as standard procedure).
- 6.6 Staff need to be aware of the usual pattern of deliveries and to be briefed of unusual deliveries. The best practice is to open letters with letter openers (and with minimum movement) to keep hands away from noses and mouths and always wash your hands afterwards. Staff should not blow into envelopes or shake them. Packages suspected of containing chemical biological or radioactive (CBR) material should ideally be placed in a double-sealed bag. (See 6.32 for definitions of CBR)
- 6.7 If a suspicious package is received in the post or hand delivered the following actions should be taken (see Appendix A, Action Card 3; items 6 – 9):
- (a) place the package/letter in isolation and away from water, sand, chemicals, or heated surfaces, naked flames or gaseous substances. It is more likely an incendiary device than a bomb i.e. designed to start a fire;
 - (b) do not shake, squeeze or open the letter or package;
 - (c) items of mail should be placed in a transparent sealed plastic bag;
 - (d) do not tamper with or move any suspect item;
 - (e) turn off air conditioners, fans, photocopiers, printers, computers and heaters within the room where the letter/package is located;
 - (f) close all windows and evacuate the room, lock all doors and leave the keys in the lock;
 - (g) place a clearly visible warding on the door;
 - (h) inform your immediate manager and the LSMS) (NB: Security Department within Secure Division), or out of hours on call manager of the situation as soon as the room is vacated;
 - (i) call the police;
 - (j) go to an isolated room and avoid other people if you can. It is vitally important that you segregate yourself and others who have come into contact with the suspicious package. REASSURE YOUR STAFF OR COLLEAGUES. It is unlikely that they are contaminated and they will get medical treatment if required;
 - (k) do not rub eyes: touch your face or other people: thoroughly wash your hands in soap and water as soon as possible.

6.8 Vehicle Bombs/Vehicle Borne Improvised Explosive Devices (VBIEDs)

- 6.8.1 Vehicle bombs are one of the most effective weapons in the terrorist's arsenal. They are capable of delivering a large quantity of explosives to a target.
- 6.8.2 Building a vehicle bomb requires a significant investment of time, resources and expertise. Because of this, the terrorist will seek to obtain the maximum impact for their investment. They generally choose high-profile targets where they can cause the most damage inflict mass casualties and attract widespread publicity.

6.9 Person-Borne Bombs

- 6.9.1 Person-borne bombs are usually, as their name implies, explosive devices carried by an individual.
- 6.9.2 These are usually carried in containers such as rucksacks or briefcases, which are chosen to blend in easily with the target surroundings. Given the requirement to be easily portable, such bombs are unlikely to weigh more than 25kg, although even an ordinary sized briefcase can contain about 12kg of explosive. A 25kg suitcase bomb could destroy a house or cause serious structural damage to larger buildings.
- 6.9.3 Terrorists often increase the effectiveness of their bombs by packing them with nails, nuts and bolts or similar items to act as shrapnel. Such weapons can have a devastating effect in a small or confined space.

6.10 Suspicious Packages

- 6.10.1 A suspicious object is an item, which may contain a bomb, which is out of place and which cannot be accounted for. Any suspicious package or box found must be treated with extreme caution, and must be reported immediately.
- 6.10.2 Unidentified parcels, packages, bags and other items left unattended for some time must be considered as suspicious and reported to the most senior person on duty, if applicable the SITE SECURITY OFFICER, and during normal working the Trust's Security Advisor in the first instance. Packages of this nature must not be touched or tampered with in any way.
- 6.10.3 Attempts must be made to identify the owner of the package. Where this fails and cause for concern remains, the Police must be called upon to advise the next possible course of action.

6.11 What You Can Do?

- 6.11.1 Operating general good housekeeping practices with effective access control of staff and visitors greatly reduces the chances of a bomb being carried onto Trust premises. Challenge people you do not recognise and ask for identification. Managers of the individual Trust sites should consider that the most effective access control is an efficient reception area. Access to side and rear entrances should be restricted to authorised persons only. Consider use of access-controlled internal doors between reception areas and offices to prevent unauthorised entry.
- 6.11.2 Introduce a visitor's book and ensure it is managed effectively – this is useful if the premises need to be evacuated and a head count required to account for all persons on the premises. All visitors should be requested to sign in and give details of their vehicle.
- 6.11.3 Regular risk assessments should be carried out to ensure that the appropriate protective security measures are in place. The Chief Executive and Security Management Director are required under the legislation to monitor and ensure compliance with these directions.
- 6.11.4 At times of high alert, baggage searches may be the only available means of protection and deterrence. Should a suspicious item be found during a search, under

Community and Mental Health Services
no circumstances should it be touched or moved in any way. The police should be informed immediately and they will ensure an appropriate response.

6.11.5 Key information and telephone numbers should be prominently displayed and readily available.

6.12 Search Plans

6.12.1 The police response to searching Trust premises would depend on their Force Incident Manager's grading of the incident. The police response will be classified as STANDARD, AMBER or RED.

6.12.2 In all cases an officer will attend the scene but the police would not normally search for a STANDARD class response. However, they would advise that staff search the premises and inform the police if anything unusual is found. Staff involved in searching the Trust's premises must be familiar with the areas they are searching and with what they would normally expect to find there, but they do not need to be experts in explosives or other devices. In particular, they should look for anything that should not be there or is out of place, and anything that cannot be accounted for. Ideally, staff should search in pairs to ensure nothing is missed.

6.12.3 Searches are also made following evacuation. In this instance, it is essential that staff liaise with the police to confirm that the building is safe for re-occupation. If a search is required, the police may need the assistance or involvement of staff, who will have a far better knowledge of the premises.

6.12.4 When preparing a search plan you should:

- (a) appoint a Search Coordinator to produce and maintain a search plan. He or she should initiate any searches and liaise with other searches;
- (b) divide the building into search sectors, each of a manageable size for one or two searches;
- (c) prioritise the important areas that need to be searched; particularly those areas open to the public, other vulnerable areas such as cloakrooms, stairs, corridors and lifts, as well as evacuation points and routes, car parks and other outside areas such as goods or loading bays;
- (d) consider how to initiate the search:
- (e) **DO NOT USE** personal radios, telephones or pagers – may well detonate the device,
 - (f) cascade by telephone, or in person may be the only viable option;
 - (g) ensure the searchers know what to do on discovering a suspicious item – under no circumstances should it be touched or moved in any way – and the police should be informed immediately (999);
 - (h) check the search plan with local police CTSA and the LSMS and practice it regularly.

6.13 Evacuation Plans

6.13.1 The purpose of evacuation is to move people away from an area where they might be at risk to a place of lesser risk. The premises may need to be evacuated because of:

- (a) a threat aimed directly at the building;
- (b) a threat received elsewhere and passed on to the Trust by the police;
- (c) discovery of a suspicious item in the building (perhaps a postal package, an unclaimed hold-all or rucksack);
- (d) discovery of a suspicious item or vehicle outside the building;
- (e) an incident to which the police have alerted the Trust.

6.13.2 Whatever the circumstances, you should inform the police as soon as possible what action you are taking.

6.13.3 The biggest dilemma facing anyone responsible for an evacuation plan is how to judge where the safest place might be. For example, if an evacuation route takes people right past a suspect device outside the Trust's building, or through an area believed to be contaminated, evacuation may not be the best of action. You might have to consider the use of protected spaces

6.13.4 A general rule of thumb is to find out if the device is external or internal to the premises. If it is within the building you may consider evacuation, but if the device is outside the building it may be safer to stay inside.

6.13.5 The decision to evacuate a building should be made by the Senior Manager on site, in consultation with the Trust's Security Co-coordinator and the police.

6.13.6 The preparation of individual site evacuation plans is the responsibility of the Local Clinical Nurse Manager and the plans should be prepared in consultation with the Trust's Local Security Management Specialist and the Estates & Facilities Office (See Appendix B; Building Evacuation Profile Template). The plans should include:

- (a) full evacuation outside the building;
- (b) evacuation of part of the building, if the device is small and thought to be confined to one location (e.g. a letter bomb found in the post room);
- (c) full or partial evacuation to an internal safe area, such as a protected space, if available;
- (d) evacuation of all staff apart from designated searchers.

6.14 Evacuation

6.14.1 The police would not advise evacuation unless a suspect package is found. The first priority is to move everybody to a place of safety. This may be achieved by external evacuation or internal sheltering.

6.14.2 The police can advise on the best option. Evacuation instructions must be clearly communicated to staff and routes and exits must be well defined. Appoint people to act as marshals and as contacts once the assembly area is reached.

6.14.3 Assembly areas should be at least 500 metres away from the incident unless otherwise agreed. In the case of most vehicle bombs, for instance, this distance would put them beyond police cordons – although it would be advisable to have an alternative about 1 km away.

6.14.4 Car parks should not be used as assembly areas. Any evacuation point should be searched and should not be near to secondary hazards i.e. glass (windows etc) or petrol supplies/sources (vehicles).

6.15 Disability Discrimination

6.15.1 Staff and visitors who have a disability should be individually briefed on their evacuation procedures. Many organisations advise the use of fire fighter lifts or 'Evac' chair for evacuating disabled staff/visitors in the event of an incident. Consider that disabilities are not just related to physical mobility (which is clearly an important factor when implementing evacuation procedures) but also include sensory loss (people with impaired vision and hearing) and those with learning disabilities. Staff should also be aware of the needs of patients/visitors who appear to be in a confused state, as well as the elderly and infirm.

6.16 Letter or Parcel Bombs

6.16.1 Evacuate the room and the floor concerned and the adjacent rooms along the two floors immediately above and below.

6.17 Re-occupancy

6.17.1 Re-occupancy must always be discussed with the police and as necessary the other emergency services. Safety remains paramount, and allowance must be made for secondary devices (bomb) vagueness of descriptions of location of suspected devices. If an explosion occurs the building structure may be unsound and damage to power and gas may make the environment unsafe. Where a crime has been committed, the building itself will be a crime scene.

6.17.2 Where re-occupancy of a clinical area is not possible the 'Emergency Accommodation Plan', will be activated within the Secure Division which is accessible to key persons within the command structure via Imogen Cloud. Other emergency arrangements will be made within local services including distributing service users across sites.

6.18 Control of the Immediate Area – Cordons

6.18.1 The area around a bomb threat incident is a crime scene and the police may need to carry out an investigation to gain material evidence. The area may also be unsafe to enter because of devices found at the scene. Inner and outer cordons may be required and the police will advise on this. This may take some time and during that period, people may be excluded from the area so that vital evidence is not lost.

6.19 Command structures

- 6.19.1 In the event of a prolonged incident the emergency services and the local authority may implement a formalised command structure.
- 6.19.2 Strategic Level – Gold Command – The Director responsible for the service where the incident occurs or out of hours the On Call Director/Chief Executive are in overall charge and responsible for formulating the Trust’s strategic response. In the event of a major incident being declared, a multi-agency Gold Control (also known as Strategic Coordination Group) may be established. This is a strategic group and will look at the wider impact of the incident and make any high level strategic decisions.
- 6.19.3 Tactical Level – Silver Command – During the normal working day a Senior manager or if the incident occurs ‘Out of Hours’ – The Director on Call will take charge of the scene of the incident and be responsible for formulating the tactics to be adopted by the Trust. Each agency involved will have a silver team operating and if a major incident team is convened within the Trust, this will be known as Silver control.
- 6.19.4 Communication between silver controls is important and the Trust may be asked to send a representative to the local authority silver control room to provide information or attend a meeting.
- 6.19.5 Operational Level – Bronze Command – The operational level staff will control and deploy the resources of the Trust within a defined area or to a specified role, implementing the tactics decided by the Tactical Level manager. Bronze is an operational control and usually refers to those actively involved in responding to the incident. If a major incident team has been convened, it is important to ensure that robust 2-way communication is established with staff operating at Bronze level. The Bronze Controller will co-ordinate their activities and oversees communication within the Incident Team.
- 6.19.6 Communication to other agencies should be done through their Silver Control – ask for the Silver Commander – as they should have a better overview of the incident than anyone working at Bronze level.

6.20 **Chemical, biological, radiological and nuclear attacks (CBRN).** Since the early 1990s, concern that terrorists might use CBR materials as weapons has been raised. ‘CBR’ is a general term that covers three distinct groups of hazards:

- (a) Chemical – Poisoning or injury caused by chemical substances, including ex military chemical warfare agents or legitimate but harmful household or industrial chemicals;
- (b) Biological – Illnesses caused by the deliberate release of dangerous bacteria, viruses or fungi, or biological toxins (e.g. ricin, a natural toxin occurring in plants);
- (c) Radiological (radioactive) – Illness caused by exposure to harmful radioactive materials contaminating the environment.

6.20.1 Much of the CBR – related activity seen to date has either been criminal or has involved hoaxes and false alarms. There have so far only been a few examples of terrorists using CBR materials. The most notable were the 1995 sarin gas attack on the Tokyo subway, which killed twelve people, and the 2001 anthrax letters in the United States, which killed five people.

6.20.2 CBR weapons have been little used so far, largely due to the difficulty of obtaining the materials and the complexity of using them effectively. Where terrorists have tried to carry out CBR attacks, they have generally used relatively simple materials. However, Al Qaida and related groups have expressed a serious interest in using CBR. The impact of any terrorist CBR attack would depend heavily on the success of the chosen dissemination method and the weather conditions at the time of the attack.

6.20.3 The likelihood of a CBR attack remains low. As with other terrorist attacks, you may not receive prior warning of a CBR incident. Moreover, the exact nature of an incident may not be immediately obvious. First indicators may be the sudden appearance of powders, liquids or strange smells within the building, with or without an immediate effect on people.

6.20.4 Good general physical and personnel security measures will contribute towards resilience against CBR incidents. Remember to apply appropriate personnel security standards to contractors, especially those with frequent access to your site.

6.21 Identifying CBR Materials in the Post

6.21.1 Terrorists may seek to use chemical, biological or radiological materials in letter bombs. It is difficult to provide a full list of possible CBR indicators because of the diverse nature of the materials. However, some of the more common and obvious are:

- (a) unexpected granular, crystalline or finely powdered material (of any colour and usually with the consistency of coffee, sugar or baking powder), loose or in a container. CBR devices containing finely ground powder or liquid may be hazardous without being opened;
- (b) unexpected sticky substances, sprays or vapours;
- (c) unexpected pieces of metal or plastic, such as discs, rods, small sheets or spheres;
- (d) strange smells, e.g. garlicky, fishy, fruity, mothballs, peppery, meaty, rotten. If you detect a smell, do not go on sniffing it. However, some CBR materials are odourless and tasteless;
- (e) stains or dampness on the packaging;
- (f) sudden onset of illness or irritation of skin, eyes or nose.

6.22 What To Do in a CBR Incident

- (a) the precise nature of the incident (chemical, biological or radiological) may not be readily apparent. Keep your response plans general and wait for expert help from the emergency services;
- (b) review plans for protecting staff in the event of a terrorist threat or attack;
- (c) remember that evacuation may not be the best solution. You will need to be guided by the emergency services on the day;

- (d) plan for the shutdown of systems that may contribute to the movement of airborne hazards (e.g. computer equipment containing fans);
- (e) ensure that external doors can be closed quickly if required;
- (f) if your external windows are not permanently sealed shut, develop plans for closing them in response to a warning or incident;
- (g) examine the feasibility of emergency shutdown of air-handling systems and ensure that any such plans are well rehearsed;
- (h) where a hazard can be isolated by leaving the immediate area, do so as quickly as possible, closing doors and windows as you go;
- (i) move those directly affected by an incident to a safe location as close as possible to the scene of the incident, so as to minimise the spread of contamination;
- (j) separate those directly affected by an incident from those not involved so as to minimise the risk of inadvertent cross contamination;
- (k) ask people not to wander off-though you cannot contain them against their will;
- (l) you do not need to make any special arrangements beyond normal first aid provision. The emergency services will take responsibility for the treatment of casualties;
- (m) in the event of a suspect CBR incident within the building, switch off all air conditioning, ventilation and other systems or items that circulate air (e.g. fans and personal computers). Do not allow anyone, whether exposed or not, to leave evacuation areas before the emergency services have given medical advice, assessments or treatment;
- (n) if an incident occurs outside the building, close all doors and windows and switch off any systems that draw air into the building;
- (o) remember to let the police know what action you are taking during any incident;
- (p) building managers should ensure that they have a working knowledge of the heating, ventilation and air condition (HVAC) systems and how these may contribute to the spread of CBR materials within the building.

7. CONSULTATION

- 7.1 This policy has been circulated to the EPRR group as well as the Local Security Management group and to the Health & Safety Committee.
- 7.2 The Trust will ensure that all members of staff are provided with the information that they require to work safely and without risk to their health. This will include information, such as the results of assessments and the appointment of various categories of competent persons, required under various pieces of legislation.

- 7.3 Consultation on health and safety matters with employees who are members of a recognised trade union will take place through the agreed channels. However; employees who are not members of a recognised trade union will be consulted with either directly or through a representative whom they have elected. This will enable the trust to meet its obligations under the Consultation with Employees Regulations 1996.

8. TRAINING AND SUPPORT

- 8.1 Aiding evacuation in the event of a bomb threat/suspicious package will be included in Fire Warden/Marshal training.
- 8.2 Development of specific Building Evacuation Profiles (See Action Card 3) will be completed by the LSMS for each division in conjunction with the building manager and service lead.
- 8.3 The evacuation procedure (Action Card 3) will be developed for each building according to the risks presented and will be held alongside the buildings Lockdown Procedure. Familiarization of staff will be the responsibility of the divisional LSMS (NB: or security department within secure division), in conjunction with the senior on site manager.
- 8.4 The Trust will undertake at least one table top exercise per year within each division. This will be organised by the Head of Risk and EPRR. All learning from these exercises will be disseminated through the divisional governance committees via the EPRR group.
- 8.5 Silver on call, will be familiarised with the policy and participate in planned exercises. LSMS responsible for each site will identify an evacuation point and instigate table top exercises. The Counter Terrorism Unit will provide training places from time to time.

9. MONITORING

What part of this policy will be monitored?	Where in the policy is it referenced	Who will carry out the monitoring	What will the frequency of monitoring be	Which group/committee will receive the monitoring reports
Evacuation plans to ensure they are adequate	6.13	Health and safety team	Annually during testing of evacuation drills	Health and safety committee
Command Structures to ensure there are no gaps in the control, elements	6.19	Head of EPRR	Annually	Health and safety Committee Quality Assurance Committee
Training and Support the completion of at least one table top exercise	8.4	Head of EPRR Head of Health and Safety	Annually	Health and safety Committee Quality Assurance Committee

10. Equality and Human Rights Analysis

Title: Bomb Threat Suspicious Package Policy

Area covered: All Trust staff except High Secure Services and secure postroom

What are the intended outcomes of this work? *Include outline of objectives and function aims*

Increase staff awareness, and identify protocols on what to do in the event of a suspicious package

Who will be affected? *e.g. staff, patients, service users etc*

Staff, service users, visitors

Evidence

What evidence have you considered?

NHS Protect guidelines, Health & Safety at Work Act

Disability (including learning disability)

Assistance will be required to enable individuals to reach a place of safety

Sex

NA

Race *Consider and detail (including the source of any evidence) on difference ethnic groups, nationalities, Roma gypsies, Irish travellers, language barriers.*

NA

Age *Consider and detail (including the source of any evidence) across age ranges on old and younger people. This can include safeguarding, consent and child welfare.*

NA

Gender reassignment (including transgender) *Consider and detail (including the source of any evidence) on transgender and transsexual people. This can include issues such as privacy of data and harassment.*

NA

Sexual orientation *Consider and detail (including the source of any evidence) on heterosexual people as well as lesbian, gay and bi-sexual people.*

NA

Religion or belief *Consider and detail (including the source of any evidence) on people with different religions, beliefs or no belief.*

NA

Pregnancy and maternity *Consider and detail (including the source of any evidence) on working arrangements, part-time working, infant caring responsibilities.*

NA

<p>Carers Consider and detail (including the source of any evidence) on part-time working, responsibilities.</p> <p>Community and Mental Health Services <i>Shift-patterns, general caring</i></p> <p>NA</p>
<p>Other identified groups Consider and detail and include the source of any evidence on different socio-economic groups, area inequality, income, resident status (migrants) and other groups experiencing disadvantage and barriers to access.</p> <p>NA</p>
<p>Cross Cutting implications to more than 1 protected characteristic</p>

Human Rights	Is there an impact? How this right could be protected?
Right to life (Article 2)	Not engaged
Right of freedom from inhuman and degrading treatment (Article 3)	Supportive of a HRBA
Right to liberty (Article 5)	Not engaged
Right to a fair trial (Article 6)	Not engaged
Right to private and family life (Article 8)	Not engaged
Right of freedom of religion or belief (Article 9)	Not engaged
Right to freedom of expression Note: this does not include insulting language such as racism (Article 10)	Not engaged
Right freedom from discrimination (Article 14)	Not engaged

<p>Engagement and Involvement detail any engagement and involvement that was completed inputting this together.</p>
<p>This policy has been circulated to the EPRR group as well as the Local Security Management group and to the Health & Safety Committee.</p>
<p> </p>
<p> </p>

<p>Summary of Analysis This highlights specific areas which indicate whether the whole of the document supports the trust to meet general duties of the Equality Act 2010</p>
--

Eliminate discrimination, harassment and victimisation

Where appropriate the policy is supportive

Advance equality of opportunity

Where appropriate the policy is supportive

Promote good relations between groups

Where appropriate the policy is supportive

What is the overall impact?

The overall impact on the implementation on this policy review is minimal

Addressing the impact on equalities

There needs to be greater consideration re health inequalities and the impact of each individual development /change in relation to the protected characteristics and vulnerable groups

Action planning for improvement

Detail in the action plan below the challenges and opportunities you have identified. *Include here any or all of the following, based on your assessment*

- Plans already under way or in development to address the **challenges** and **priorities** identified.
- Arrangements for continued engagement of stakeholders.
- Arrangements for continued monitoring and evaluating the policy for its impact on different groups as the policy is implemented (or pilot activity progresses)
- Arrangements for embedding findings of the assessment within the wider system, OGDs, other agencies, local service providers and regulatory bodies
- Arrangements for publishing the assessment and ensuring relevant colleagues are informed of the results
- Arrangements for making information accessible to staff, patients, service users and the public
- Arrangements to make sure the assessment contributes to reviews of DH strategic equality objectives.

For the record

Name of persons who carried out this assessment:

Carlton Brooks

Date assessment completed:

04 February 2019

Name of responsible Director:

Elaine Darbyshire

Date assessment was signed:

04 Feb. 19

Appendix A – Action Cards

Action Card: 1;

Protective Marking: Restricted when Completed

Form 5474

ACTIONS TO BE TAKEN ON RECEIPT OF A BOMB THREAT

- 1 Remain calm and talk to the caller
- 2 Note the caller's number if displayed on your phone
- 3 If the threat has been sent via email or social media see appropriate section below
- 4 If you are able to, record the call
- 5 Write down the exact wording of the threat:

When Where What How Who Why Time

ASK THESE QUESTIONS & RECORD ANSWERS AS ACCURATELY AS POSSIBLE:

1. Where exactly is the bomb right now?	
2. When is it going to explode?	
3. What does it look like?	
4. What does the bomb contain?	
5. How will it be detonated?	
6. Did you place the bomb? If not you, who did?	
7. What is your name?	
8. What is your address?	
9. What is your telephone number?	
10. Do you represent a group or are you acting alone?	
11. Why have you placed the bomb?	
Record time call completed:	

Protective Marking: Restricted when Completed

INFORM BUILDING SECURITY/ COORDINATING MANAGER

Name and telephone number of person informed:

DIAL 999 AND INFORM POLICE

Time informed:

This part should be completed once the caller has hung up and police/ building security/ coordinating manager have all been informed

Date and time of call:

Duration of call:

The telephone number that received the call:

ABOUT THE CALLER:

Male	Female	Nationality?	Age?
<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>

THREAT LANGUAGE:

Well-spoken	Irrational	Taped	Foul	Incoherent
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

CALLER'S VOICE:

	Calm	Crying	Clearing throat	Angry	Nasal	
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Slurred	Excited	Stutter	Disguised	Slow	Lisp	*Accent
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Rapid	Deep	Familiar	Laughter	Hoarse	Other (please specify)	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		

*What accent?

If the voice sounded familiar, who did it sound like?

BACKGROUND SOUNDS:

	Street noises	House noises	Animal noises	Crockery	Motor
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Clear	Static	PA system	Booth	Music	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Voice	Office machinery	Other (please specify)			
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			
Factory machinery					
<input type="checkbox"/>					

Action Card 2

ACTIONS TO BE TAKEN ON RECEIPT OF A BOMB THREAT SENT VIA EMAIL OR SOCIAL MEDIA

- 1 DO NOT reply to, forward or delete the message
- 2 If sent via email note the address
- 3 If sent via social media what application has been used and what is the username/ID?
- 4 Dial 999 and follow police guidance
- 5 Preserve all web log files for your organisations to help the police investigation (as a guide, 7 days prior to the threat message and 48 hours after)

Signature: Print Name: Date:.....

SAVE AND PRINT – HAND COPY TO POLICE AND SECURITY/ COORDINATING MANAGER

Retention Period: 7 years

Action Card 3

IMMEDIATE ACTIONS ON SUSPICION OF EXPLOSIVE DEVICE/BOMB THREAT

SUSPECTED EXPLOSIVE DEVICE/BOMB THREAT – use as checklist		
Activated under direction from building manager/site manager		
Role: To initiate the evacuation of staff , service users and visitors to a place of safety		
STEP	Tasks	Tick when Complete
1	STAY CALM: On being aware of possible bomb threat, or find of a suspect package	
2	DO NOT TOUCH OR MOVE THE OBJECT , however if you inadvertently open a suspect package place gently on the floor and retreat.	
3	Call 999 (Police) Do not use MOBILE PHONE communication as it may trigger the device. Use a landline only	
4	Inform the senior manager for the area (In-hours) (Silver on Call out of hours). Give as much information as to the suspect packages location.	
5	Corporate services: Contact Gold on call via switchboard.	
6	Evacuate immediate area , move well away from glassed areas. Where available utilise Fire Wardens/Marshalls to aid evacuation and sweep the building.	
7	Close doors behind you – if possible place barrier e.g. metal cupboard between door and device. Do not lock the door.	
8	If possible open windows. Leave an external door open to allow access.	
9	Evacuate to a safe distance 500 meters from the building. Refer to local bomb threat ‘evacuation profile’, for assembly point (external/internal). (NB: the Fire evacuation muster point is too close to the building.)	
10	Prevent people entering area – if necessary shout your warning. Place no entry notices on exit doors.	
11	Leave area as in steps 6-9.	
12	Only re-enter the building when police indicate that it is safe to do so	
NOTES		

Appendix: B

Bomb Threat / Suspicious Package Building Evacuation Profile Template

Bomb Threat/Suspicious Package Evacuation Profile	
Building/Site Name:	
Address:	
Date of Survey:	
Site Plan / Area Map Attached:	
Survey Completed by:	
Characteristic	Information
Search Zones identified on building Map	
External Evacuation Area (Mark on area map – google maps)	
Internal Shelter Area: Safe area to evacuate internally (Large inpatient sites – ground floor)	
Contact details Name, number and designation	
Potential Hazards adjoining building e.g. chemical plant, inflammables	
Contact Details of Close Neighbours Provide to police to enable their safety	
NB: To be attached to Lockdown procedure which contains site and building profiles	