
Suspect Packages Policy

Solent NHS Trust policies can only be considered to be valid and up-to-date if viewed on the intranet. Please visit the intranet for the latest version.

Purpose of Agreement	To provide Guidance to staff on how to deal with the receipt of a bomb threat over the telecommunications system or how to ensure evacuation in the event of a discovery of a suspect package or device
Document Type	<input checked="" type="checkbox"/> Policy <input type="checkbox"/> SOP <input type="checkbox"/> Guideline
Reference Number	Solent NHS T/Policy/RK09
Version	Version 3
Name of Approving Committees/Groups	Policy Steering Group, Management Meeting
Operational Date	August 2020
Document Review Date	August 2023
Document Sponsors (Name & Job Title)	Chief Finance Officer/ Deputy CEO [Security Management Director SMD]
Document Manager (Name & Job Title)	Accredited Security Management Specialist (ASMS)
Document developed in consultation with	Health & Safety Committee
Intranet Location	Business Zone > Policies, SOPs and Clinical Guidelines
Website Location	Publication Scheme
Keywords (for website/intranet uploading)	Suspect Package, Explosives, Bomb Threat, Hoax Call, Improvised Explosive Device IED, Chemical, Biological, Radioactive, Nuclear (CBRN) Terrorism, Policy, RK09

Review Log

Include details of when the document was last reviewed:

Version Number	Review Date	Lead Name	Ratification Process	Notes
1				
2				
3	February 2020	Stuart Francis	Policy Steering Group	3 yearly update

Amendments Summary:

Amend No	Issued	Page(s)	Subject	Action Date
Version 2	Nov 16		Suspicious Package Response Policy will now be known as Policy for Suspect Packages Policy e-written	Nov 16
Version 3	December 2019	6, 7 8, 13, 22	Renamed policy to Suspect Packages Policy Amendments to Run Hide Tell / Threat levels NPCC run hide tell video location General update of advice and guidance	February 2020 Policy Steering Group

Executive Summary

This policy gives comprehensive guidance to all Solent staff, including managers & Directors, to make them aware of the correct procedures to follow on receiving or discovering a suspect package, telephone warning or Bomb Threat. The Policy when followed is an essential part of ensuring the right people are notified and that the safety and security of staff and patients utilising Solent NHS Trust facilities is first and foremost considered.

Table of Contents

	Suspect Packages Policy	Pages
1	Introduction & Purpose	4
2	Scope & Definitions	4
3	Process and Requirements	6
4	Roles & Responsibilities	10
5	Training	11
6	Equality Impact Assessment and Mental Capacity	12
7	Success Criteria / Monitoring Effectiveness	12
8	Review	12
9	References to web sites	12
10	References to other documents	13
11	Glossary of definitions	13
	Annex A – Information to be taken on receipt of a bomb threat or discovery of a suspect package	14
	Annex B – Chemical or Biological Attack	17
	Annex C – Information Required by the Police on Arrival	19
	Annex D – Recommended Safe Distances	20
	Annex E – Bomb Threat Flow Chart	21
	Annex F – Suspicion letter / package Flow Chart	22
	Annex G – Equality Impact Assessment	23

Suspect Packages Policy

1. INTRODUCTION & PURPOSE

1.1 Introduction & Purpose

- 1.1.1 This policy aims to support staff in how to safely and efficiently deal with the discovery of a suspect package/device, or the threat of one across the Telecommunications network it will provide staff with confidence to quickly report any findings to the relevant people. Swift action will protect staff, patients and the public who may be using Trust premises.
- 1.1.2 Solent NHS Trust attaches the greatest importance to, and concerns for, the safety of all its employees, service users and other persons on Trust property. Solent NHS Trust has a statutory duty to provide a safe place of work and, in order to fulfil this duty; there is a requirement to make plans for dealing with suspect packages/devices and bomb threats. A package/device could be planted on Trust property, or received via the postal system.
- 1.1.3 The policy helps to ensure that effective procedures are in place and are clearly understood by all to secure, so far as is reasonably practicable, the Health, safety and welfare of all employees, services users and Third Parties to Trust facilities.
- Communicate and promote the Trusts commitment in minimising the risks to employees, service users and visitors from acts of unlawful interference involving improvised explosive (IED) or Chemical, Biological, Radioactive or Nuclear (CBRN) devices.
 - The creation of a standard threat response.
 - The creation of a pro-security culture – The promotion of a culture where security is the responsibility of every member of staff.
 - Provide a comprehensive framework that all employees can follow if they receive a bomb threat or have a reason to suspect there is a suspicious package/device on site.

2. SCOPE

- 2.1 This policy applies to bank, locum, permanent and fixed term contract employees (including apprentices) who hold a contract of employment or engagement with the Trust, and secondees (including students), volunteers (including Associate Hospital Managers), Non-Executive Directors, and those undertaking research working within Solent NHS Trust, in line with Solent NHS Trust's Equality, Diversity and Human Rights Policy. It also applies to external contractors, Agency workers, and other workers who are assigned to Solent NHS Trust.
- 2.2. **National Terrorist Threat Levels**
- 2.2.2 The current 5 levels of terrorist threat as published by the UK Security Services for the UK are as follows;

Threat Level		Response	
Critical	An Attack is Expected Imminently	Exceptional	Maximum Protective security Measures to meet specific threats and to minimise vulnerability and risk. Critical may also be used if nuclear attack is expected
Severe	An Attack is Highly Likely	Heightened	Additional and sustainable protective security measures reflecting the broad nature of the threat combined with specific business and geographical vulnerabilities and judgements on acceptable risk
Substantial	An Attack is strong Possibility		
Moderate	An attack is possible but not likely	Normal	Routine Protective security measures appropriate to the business concerned.
Low	An Attack is unlikely		

2.2.2 These levels are set by the Joint Terrorism Analysis Centre (JTAC) and the Military Security Service (MI5).

2.2.3 Threat levels do not have an expiry date. They can change at any time as different information becomes available to security specialists. This is then communicated by the Government services to their various chosen media outlets to make the public aware.

2.2.4 If the incident is happening in real time then please urgently call the Police on (9) 999. Alternatively contact the **TERRORIST HOTLINE – 0800 789 321**

2.2.5 If it is retrospective or deemed not urgent but you have suspicions, information or concerns regarding something you have seen relating to terrorism Police can be contacted on 101 for further information

2.3 Emergency Services Major Incident Command Structure

2.3.1 During a major incident, such as the discovery of a suspect package/device, all three emergency services would be involved, or placed on standby. All requests will come via the on scene manager who will often be a Police officer of the rank of sergeant or above, this could in some cases in the early stages be a Police Constable acting on behalf of the on duty Sergeant until their arrival, or the arrival of an area inspector on scene. Staff must follow all commands or requests placed on them by Police whose structure will follow:

1. Strategic Command – GOLD (chief inspector and some cases a superintendent)
2. Tactical Command – SILVER (inspector or chief inspector)
3. Operational Command – BRONZE (sergeant or inspector)

Please Refer the police to any Incident response plans, BCP and provide contact details of any on call manager or director who must be included in all decisions. An incident control room if opened up must be updated regularly.

2.3.2 RUN HIDE TELL

Run, Hide, Tell is a government initiative providing guidance to small businesses, companies as well as NHS Trusts to be prepared for terrorist attacks.

The information is collated and provided by Police / MI5 and (JTAC) Joint terrorist Analysis Centre for people to follow during any Terrorist attack or incident to try and preserve as much life as possible

Run: To a place of safety, this is better than trying to surrender or negotiate

Hide: It is better to hide than confront, barricade yourself in, turn phones to silent and use only when it is safe to do so.

Tell: Call the police by gaining an outside line and Calling **999**

2.3.3 The NPCC National Police Chiefs Council

The NPCC provides information as well as a brief video for each organisation to watch showing the need for the Run Hide Tell campaign. This is provided for staff to watch and be aware of marauding knife and weapons attacks in their organisation's planning and response to an attack.

The video can be found at:

www.npcc.police.uk/npccBusinessAreas/WeaponAttacksStaySafe.aspx

3. PROCESS/REQUIREMENTS

3.1 The Trust will comply with the Civil Contingencies Act 2004, the Department of Health, Emergency Planning Guidance, and guidance from the Centre for the Protection of National Infrastructure (CPNI) as a priority 1 responder, please see glossary for description of Priority 1.

3.1.1. Although there is no specific or direct threat to the NHS or its properties and staff trusts should still be aware of the risk from Improvised Explosive Devices (IEDs), suspect packages and hoax phone calls. The action on discovering/receiving information of a device and the disruption to the day to day running of Solent services it would cause. (**Annex A**)

3.1.2 Swift, calm decision making and prompt notification to Directors or on call management will result in a suitable outcome to the situation.

3.2 Types of Devices/Threats

3.2.1 An IED usually requires four (4) elements for a successful detonation;

1. Explosive
2. Initiator (Timer, mobile, pressure pad etc.)
3. Power
4. Detonator

- 3.2.2 It is impossible to state the shape or size of an IED as it is only limited to the imagination of the maker. It is essential therefore that any suspicious package/item left unattended should be treated with care and extreme caution, if any of the above elements is seen inside or protruding from it.
- 3.2.3 Chemical or Biological Threat- The advice offered in 'Suspicious Letters, Parcels or Suspected Bombs – The Tell Tale Signs', is applicable to IEDs as well as chemical or biological agents. Advice specific to chemical or biological threat is contained in (**Annex B**).
- 3.2.4 Suspicious Letters/Packages Parcel Bombs - These types of devices are designed to kill or seriously maim and are triggered when opened. (Remember, this item has been through the delivery service; chances are it will not be set off by movement or pressure). However, the danger posed by these types of devices should not be underestimated.
- 3.2.5 The 7 S's Tell Tale Signs
1. **Shape** – Is the parcel evenly balanced? Is there stiffening – the feel of cardboard or metal? Is there an unusual outline if held up to the light?
 2. **Stamp** – Is the postmark familiar? Are there no stamps or an excessive use of stamps – disproportionate to the weight? Is it correctly addressed?
 3. **Size** – Single page envelopes or reports, which are uniform and have balanced appearance, are unlikely to be suspect. Explosive or incendiary items will usually have some bulk, possibly disguised in a jiffy bag or postal tube. If the weight seems excessive for the size it may be suspect.
 4. **Smell** – Some explosives have a distinctive aroma (nitro-glycerine toluene's can smell of marzipan or almonds. Homemade may have more of a chemical odour) but this may be masked by perfume or aftershave.
 5. **Stain** – Some explosives can sweat or ooze liquid, causing oily or greasy marks on the packaging. Some powder could be seen covering the exterior of the package
 6. **Seal** – If it is a device the package will be well sealed and secured with staples, tape etc to prevent it coming open in transit. Often the packages are sealed in such a way that the recipient automatically attempts to open it at the 'easier', and most harmful, end.
 7. **Sender** – If in doubt, check with the sender. If there are no visible postmarks or return address, check with the addressee – are they expecting package?
- 3.2.6 Actions on discovery of a suspect package
- Do not attempt to open it.
 - Do not shake, prod or squeeze it.
 - If possible, take a photo of the package, consider putting phone in to Airplane Mode if you are within the cordon of 20 Metres (Airplane Mode switches the phone signal off to prevent inadvertent activation of any suspect package) (include in any photo the recipient's name and address) as well as any other markings take a couple of photos to be sure.
 - Place the package carefully on the floor in an open space and clear the area. Try to mark it with a cone or obvious object so police are able to locate it safely.
 - Inform the senior person present.
 - Call Police via an outside line on: **999**.
 - (**See Annex A to C**) for information required by police prior to and on arrival

ALWAYS USE A LANDLINE WHERE POSSIBLE – IF USING A MOBILE, MOVE A SAFE (see Appendix D) DISTANCE FROM THE DEVICE. Consider Skype if time allows as far away as practicable but consider Annex E below and the safe distances section of this report. **(Found at Annex D)**

3.2.7 Vehicle Borne IEDs (500 Metres Cordon)

3.2.8 A vehicle borne IED (VBIED), or car bomb, is designed to inflict maximum damage to property and cause mass casualties. Recommended safe distances **(Annex D)** must be strictly observed if dealing with such a device.

3.3 **Dealing with Telephone Warnings**

3.3.1 **All bomb warnings whether believed to be a threat or not must be taken seriously.**

3.3.2 In recent years hoax calls have substantially exceeded genuine warnings; the correct procedure must be followed to ensure the safety of staff, service users and visitors. Even a known hoax call must be reported to the Police as it is a criminal offence contrary to Section 51 of the Criminal Law Act 1977.

3.3.3 Reception(s), call centres and complaints departments are the most likely to have to deal with a telephone warning, however, employees extension numbers may be known therefore any employee could receive such a call.

3.3.4 Actions to complete when receiving a Threat via the Telephone and Skype or Mobile (See Annex A)

3.3.5 In all cases, whether or not the threat is considered credible, the following actions must be taken by the person receiving the call:

- Inform/signal a colleague of the potential emergency
- Inform the senior person present immediately
- Inform the Police immediately using 9 - 999
- Complete the questionnaire at (Annex A) during the call or as soon as practical after. Try to take down all the information and ask some simple questions if the caller allows but only after the details have been gleaned from them.
- Leave the line open, **do not hang up**. This will help the Police ascertain where the call originated from
- Contact Trust on call manager and/or on call executive director as soon as possible

3.4 **Evacuation (including horizontal evacuation)**

3.4.1 The four types of evacuation are:

Stage 1	Horizontal evacuation from the sub compartment where the incident originates to an adjoining sub compartment or compartments
Stage 2	Horizontal evacuation from the entire compartment where the incident to an adjoining compartment on the same floor
Stage 3	Vertical evacuation to a lower floor substantially remote from the floor of the origin of the incident (minimum 2 floors below) or to the outside
Stage 4	Full evacuation

- 3.4.2 The responsibility for making the decision to evacuate will rest with the senior manager/director on call, although the Police will advise, and in some circumstances overrule any decision made as they will always have primacy.
- 3.4.3 In the event of a decision being made to evacuate it should follow previously planned procedures i.e. fire evacuation. Ensure muster points are searched for secondary devices and where possible use alternative muster points.
- 3.4.4 The full evacuation or Horizontal evacuation route should take into consideration the location of the package/device. You do not want staff, patients and visitors evacuating past the suspect device. Direct them away from the package, and where possible, use the natural cover of buildings to shield people from any potential blast.
- 3.4.5 Three main courses of action are possible when in receipt of a bomb warning or on discovering a suspect package. Which one is chosen depends on the dynamic risk assessment of the threat/package received.

The options are;

1. Do Nothing – This option should only be adopted if the senior person present is absolutely sure that it is a malicious call or that the package/device is safe. If there is the slightest doubt, option 2 or 3 should be adopted.
 2. Search, then evacuate if necessary – If a suspect package is discovered all building occupants will be evacuated to the agreed muster points (Remember, look for secondary devices at the muster points).
 3. Immediate Evacuation – If a call is received/package is found and it is considered to be authentic, there is a case for evacuating the building without delay.
 - Where possible doors & windows should be left open
 - Lights should be left on to assist any subsequent search
 - All machinery should be shut down where possible
 - Do not stop to collect Personal belongings
 - Lifts may be used by individuals if they have deemed it safe to do so
 - Where possible, do not use a mobile phone within the vicinity of a suspect device
- 3.4.6 The alternative to the traditional evacuation is horizontal evacuation. The benefit of this is that staff, patients and visitors are not exposed to the elements; and those requiring greater levels of care can be supported more easily.
- 3.4.7 When assessing whether you should conduct a full evacuation or horizontal evacuation, the size of the device, location and buildings structure must be taken into consideration.
- 3.4.8 *Please refer to the Flow charts for Bomb Threat and Suspect Package (Annex E and F)*

3.5 Safe Distances

- 3.5.1 There are no specific rules when it comes to safe distances to evacuate away from a suspected IED; a lot of it will depend on the size of the device, type of explosive and what it is packed with i.e. ball bearings, nails, human/animal excrement etc.
- Always evacuate out of 'line of sight' to the device

- Where possible, use the natural cover of buildings to protect yourself
- Shrapnel can travel up to 4000 meters per second so where possible evacuate in the opposite direction from the device

Please see (Annex D) for recommended safe distances

3.6 Standing Down

- 3.6.1 Calling an end to the incident will be the responsibility of the senior Police person present. They will inform the duty director who will disseminate the information to all areas/staff involved.
- 3.6.2 An immediate 'hot' debrief should be carried out by the Incident Control Officer (Police) to capture any issues and to formally stand down all emergency services who responded.
- 3.6.3 A formal debrief will be conducted within four (4) weeks of the incident to capture any areas for improvement or good practise which can be incorporated into the policy or local plans.

3.7 The Media

- 3.7.1 Under **NO** circumstances will staff talk, or divulge information of any incident, to the media; this could be considered a criminal offence or disciplinary matter. All questions should be directed to the Trust's Corporate Communications Team. Information disclosed without prior authority could jeopardise future investigations into the incident.

3.8 Occupational Health and Wellbeing Team

- 3.8.1 Being involved in a major incident such as a bomb threat/suspect package (be it a hoax or real) is likely to have a psychological or psychosocial impact on those persons involved. All staff should recognise the need for appropriate counselling and support structures and try to be aware of the signs of Post-Traumatic Stress in themselves and their colleagues.
- 3.8.2 All staff involved should receive/be offered counselling after such an incident. Staff should either contact their own GP or speak with the Trusts Occupational Health Department, Staff should be provided with the NHSE Trauma leaflet

4. ROLES AND RESPONSIBILITIES

- 4.1 **The Chief Executive Officer** has ultimate responsibility for the management of security and safety within the Trust. This responsibility includes ensuring the aims and objectives of this policy are met and ensuring that adequate resources are made available to the relevant people at the relevant time.
- 4.2 **Accredited Security Management Specialist the (ASMS)** is responsible for the update, training and review of this policy and to assist security and reception staff who, when required, will activate the procedures within this policy, the ASMS will.

- Minimise the effect/disruption as much as is reasonably possible in the circumstances
- Reduce where possible the chance of injury/death to employees, service users and visitors.
- Increase the chance where possible of catching the perpetrator, by ensuring good evidence continuity.
- To seek Bespoke Training for Line managers and Premises managers to provide onward training to appropriate staff on what to do with discovery of Suspect packages and Telephone Threats.

4.3 **Line Managers, Premise managers**, are responsible for ensuring that they have a good working knowledge of this policy. They will be responsible for:

- Day-to-day work activities under their control are carried out with full regard to this policy.
- They must ensure that all Staff (within Call centres, Complaints departments, Reception desks including management and line managers and Receipt and Distribution Teams / goods in) undertake bespoke training in how to deal with suspect packages when discovered, and know who to call in the event of an emergency.

4.4 **Employees** must be made aware of the risk from Improvised Explosive Devices (IEDs), suspect packages and hoax phone calls.

- Familiarise themselves with this policy
- Familiarise themselves with the action to take to be taken on discovering/receiving information of a device
- Report all Incidents via Ulysses incident management system
- To consider looking at the Run Hide Tell Video (refer to section 2.3.3)

4.5 **The Trust** The trust must ensure the safe and secure management of post and provide proper storage facilities for the correct handling of any mail and the subsequent receiving of suspect packages. This will ensure that suspect mail is contained safely and securely in proper facilities. All staff within Solent could receive a call or discover a package so therefore must have a good working knowledge of this policy

4.6 **Security Management Director (SMD)** The SMD role within Solent is taken over by the Finance Director and as such has overall responsibility for any Security

4.6 **Occupational Health and Wellbeing Team will advise on:**

- Preventative and rehabilitative measures,
- Psychosocial support
- Purchase and installation of any specialist equipment,
- Fitness to work phased returns and or redeployment.
-

5. TRAINING

5.1 Training in Suspect packages will be provided to on call managers, premises managers and reception and admin staff who deal with suspect package incidents or Post and

deliveries. Training will be provided by an outside agency specialising in bespoke training of this type. To ensure key staff are familiar with the requirements relating to suspect packages a 'Basic Suspect Package and Bomb Threat Awareness' presentation has been developed and is provided to key staff in advance of their formal training session and will be provided to new staff as part of their local induction. This presentation is available on the SolNet page for security.

- 5.1.1 Any Training in suspect packages must be renewed every three (3) years to ensure that knowledge and ability is maintained.
- 5.1.2 Any alerts relating to devices must be shared with all trained staff to ensure their knowledge of current devices is kept up to date.

6. EQUALITY IMPACT ASSESSMENT AND MENTAL CAPACITY

- 6.1 This policy has no identified no significant equality or diversity issues (*please see Annex G*)

7. SUCCESS CRITERIA / MONITORING EFFECTIVENESS

- 7.1 A review of the policy and procedures will be conducted following any incident where a suspect package/device is discovered, or a threat received. Any issues/findings resulting from any debrief/investigation will be incorporated in an updated version of the policy.
- 7.2 Premises Managers are to review local procedures to comply with all relevant policies involving suspect packages/devices.
- 7.3 The ASMS will continue to monitor advice from the relevant agencies on the ever-changing threat from suspect packages to ensure that the most up to date information is available.
- 7.4 The ASMS will ensure the changing of any guidance is updated on the policy as soon as practicable.
- 7.3 All non-compliance of this policy must be reported to the ASMS via Ulysses.
- 7.4 ASMS to check Terrorist Hotline Number Annually to ensure that the contact number is current.

8. REVIEW

- 8.1 This document may be reviewed at any time at the request of either at staff side or management but will automatically be reviewed 3 years from initial approval and thereafter on a triennial basis unless organisational changes, legislation, guidance or non-compliance prompt an earlier review.

9. REFERENCES TO WEB SITES

The Civil Contingencies Act 2004 (priority 1 responders)
<http://www.legislation.gov.uk/ukpga/2004/36/contents>—————

Centre for Protection of National Infrastructure (CPNI)

<https://www.cpni.gov.uk/>

Government Bomb Threat Guidance 2016 (latest available as of 23/10/2019)

<https://www.gov.uk/government/publications/bomb-threats-guidance>

2018 Government Policy: Counter Terrorism (CONTEST)

<https://www.gov.uk/government/publications/counter-terrorism-strategy-contest>

NHS England – Emergency Preparedness, Resilience & Response (EPRR)

<https://www.england.nhs.uk/ourwork/epr/>

Public Health England (PHE) CBRN Incidents: Clinical Management & Health Protection

<https://www.gov.uk/government/organisations/public-health-england>

Homeoffice.gov.uk/terrorism

<https://www.gov.uk/terrorism-national-emergency>

National committee for warning the public of key information Nscwip.info

<https://www.gov.uk/government/groups/national-steering-committee-on-warning-informing-the-public>

10. REFERENCE TO OTHER DOCUMENTS

Incident Response Plans

Business Continuity Plans

Emergency Lockdown Policy

Fire Safety Policy

Security Management Policy

Risk Management Policy

Evacuation of Mental Health Wards Procedure

National Security Strategy 2010-2015 (latest available as of 23/10/2019)

Solent NHS trust HAZMAT SOP link

Health and Safety Policy

11. GLOSSARY OF DEFINITIONS

ASMS (Accredited Security Management Specialist)

CPNI (Centre for Protection of National Infrastructure)

NPCC (National Police Chiefs Council)

MIS (Military Intelligence 5)

EPRR (Emergency Preparedness, Resilience and Response)

NHSE (NHS England)

PHE (Public Health England)

SMD (Security Management Director)

JTAC (Joint Terrorism Analysis Centre)

IED (Improvised, explosive, device)

CCA (Civil contingencies Act (Priority 1 responder anyone within the Civil contingencies act that is an NHS trust Acute or Community Provider of services aligned to an LRF)

CBRN (Chemical, Biological, Radiological, Nuclear)

Annex A

INFORMATION TO BE TAKEN ON RECEIPT OF A BOMB THREAT OR DISCOVERY OF A SUSPECT PACKAGE

1. If a call is received or a package found Remain calm
2. Talk to the Caller and remember to note the callers number if displayed on your phone.
3. Record all details of the call, and write down the exact words of the threat
4. Note down any identifiable features of the package using the 5WH
5. Note the location and the route to take to get to it.

5WH: What When Where Why Who How + Time

Provide the following information surrounding any caller / Suspect Package and record the answers as accurately as possible;

Where exactly is the bomb right now?

Have you been told when it is likely to explode?

What does it look like?

What does the bomb contain?

How will it be detonated?

Who placed the bomb there?

What is your name?

What is your address?

What is your phone number?

Do you represent a group or are you working alone?

Why have you placed the bomb?

Have you been provided with a code word?

INFORM SENIOR PERSON/BUILDING MANAGER

Name and telephone number of person informed:

DIAL 999 – POLICE INFORMED

Time informed:

Call Details:

Date:

Time:

Duration:

About the Caller:

Male

Female

Accent

Child

Threat Language:

- Well-Spoken
- Irrational
- Taped
- Foul
- Incoherent

Callers Voice:

- Calm
- Crying
- Angry
- Nasal
- Slurred
- Excited
- Stutter
- Disguised
- Slow
- Lisp
- Accent
- Rapid
- Deep
- Familiar
- Laughter
- Hoarse
- Other

Specify -

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

Background Sounds:

- Street Noise
- House Noise
- Animals
- Crockery
- Motor
- Clear
- Voices
- Static
- PA system
- Music
- Machinery
- Office
- Other:

Specify -

Remarks:

Additional Notes:

Print Name.....

Signature.....

Date.....

Annex B

CHEMICAL OR BIOLOGICAL ATTACK

It is not thought that the NHS is at particular risk from a terrorist attack although the possibility of an individual carrying out an attack cannot be ruled out. The following advice is therefore offered.

Remember that any package will already have undergone some fairly rough handling by the delivery service. The package will also have been prepared with the intention that it should reach its intended target (it should therefore be reasonably well wrapped). If there is any specific cause for concern, consider checking all mail for suspicious signs before starting to open it.

At all times;

- Make sure that employees remain aware of the potential threat
- Ensure that items that give cause for concern are investigated
- Confirm employees know what action to take immediately, in the event of a suspicious Package being opened
- Remain vigilant

During times of heightened concern or the result of an increase in the Alert State, the following Actions should be considered;

- Open all letters and packages with care, trying not to spill any contents
- Have PPE available to staff e.g. gloves, dust masks and eye protection
- Ideally, have available an airtight container in which to place any suspicious letter or package.

Suspicious Packages – Unopened

On identifying a suspicious package, investigate & record all relevant information;

- Who/where did it come from?
- How/who delivered it?
- Why is it suspicious?
- Has it been well sealed?
- Are contents uneven?
- Are there an excessive number of stamps for the weight of the package?

‘Actions on’ if Still Suspicious

If there are sufficient reasons to be concerned, the following action should be taken;

- Place package in a sealed bag or container
- Close the windows and evacuate the room. Restrict access to the room
- Informing senior person present
- After suitable investigation and consideration, if concerns remain, contact then Police via 101 or 999

Suspicious Package – Open

If you open a letter or package and find a suspicious substance (which may have been released), take the same actions as listed above but, ensure that all employees who were in the area at the

time are identified, isolated and receive a medical check, (chances are it is entirely innocent or a hoax). In addition, and if safe to do so:

- Close all fire doors
- Close all windows in the rest of the building
- Evacuate the building unless instructed otherwise
- Call the Police
- Gain medical advice

Exposure to Contaminated Material

If you think you may have been exposed to contaminated material:

- Do not overreact
- Do not touch eyes, nose or other parts of the body
- Wash hands in soapy warm water
- Avoid contact with persons not in the immediate vicinity
- Avoid moving outside of the contained location
- Keep all persons possibly exposed to the material together, away from others and available for possible medical examination

REMEMBER:

Do carry out procedures/investigation before alerting the Emergency Services

It is far more likely that the package is a hoax – **DO NOT PANIC**

Annex C

Information Required By Police on Arrival

FIVE Cs

C ONFIRM	
C LEAR	
C ORDON	
C ONTROL	
C HECK	







Information for Explosive Ordnance Disposal (EOD) Officer

Five Ws

W hat	
W here	
W hen	
W hy	
W ho	

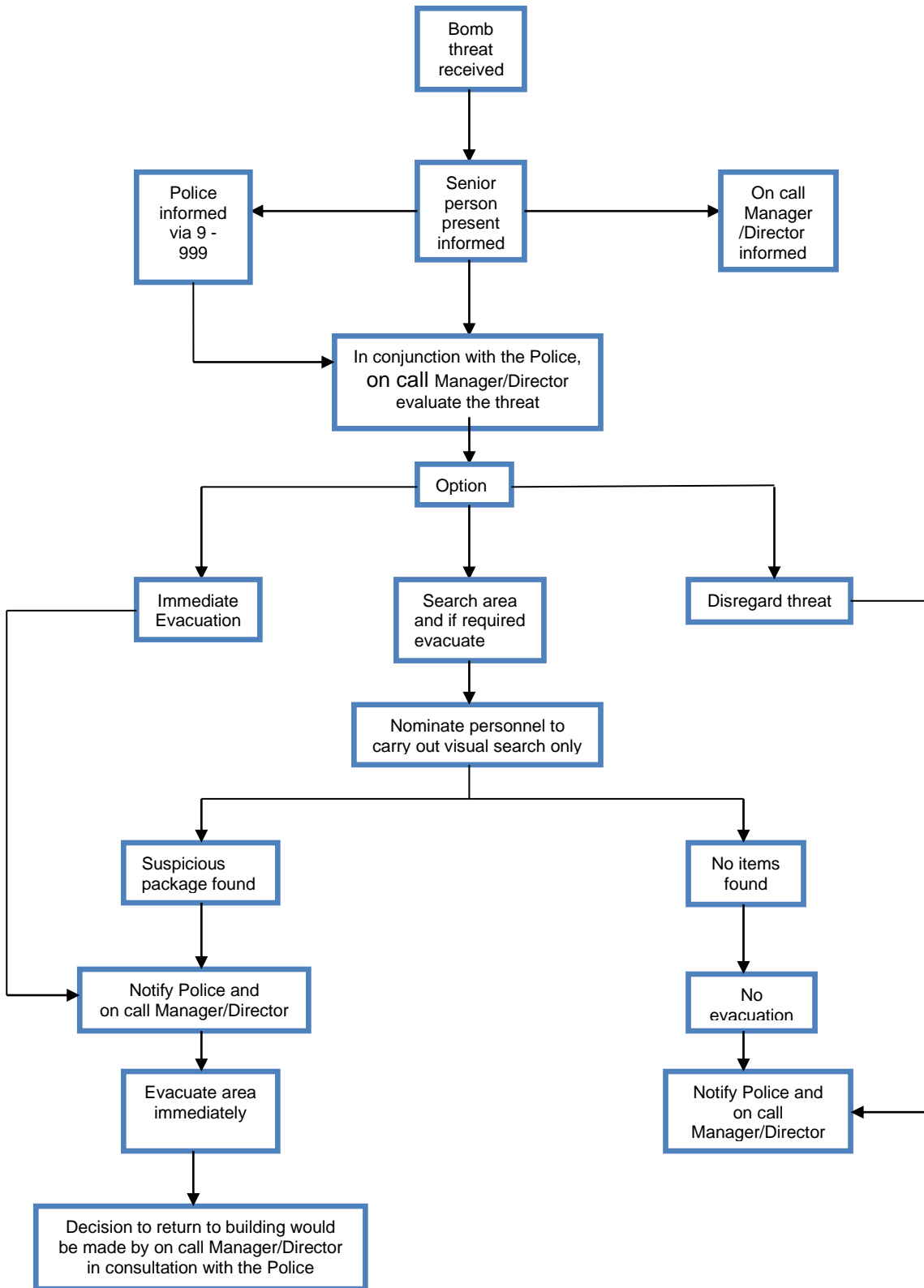
Annex D

Recommended Safe Distances

Threat Description	Explosive Capacity	Building Evacuation Distance	Outdoor Evacuation Distance
 <p>IED</p>	5lbs/2.3kg	70ft/20m	850ft/259m
 <p>Suitcase / Bag</p>	50lbs/23kg	150ft/46m	1,850ft/564m
 <p>Car</p>	1000lbs/454kg	400ft/122m	1,500ft/457m
 <p>Bus</p>	4,000lbs/1814kg	600ft/183m	2,750ft/838m
 <p>Small / Medium Lorry</p>	10,000lbs/4,536kg	860ft/262m	3,750ft/1,143m
 <p>Articulated Lorry</p>	60,000lbs/27,216kg	1,500ft/457m	7,000ft/2,134m

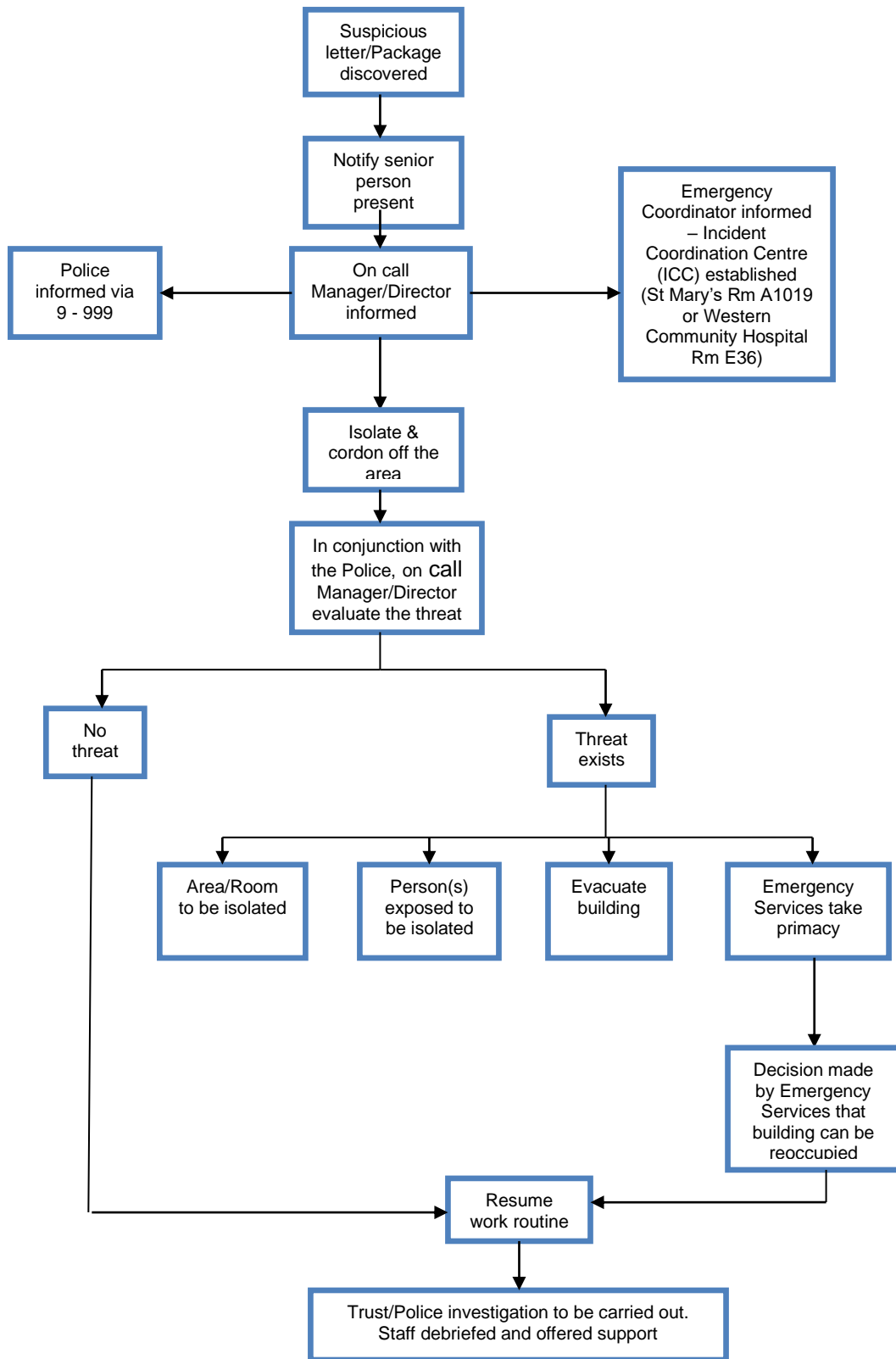
Annex E

Bomb Threat Flow Chart



Annex F

Suspicious Letter/Package



Annex G

Equality Analysis and Equality Impact Assessment

Equality Analysis is a way of considering the potential impact on different groups protected from discrimination by the Equality Act 2010. It is a legal requirement that places a duty on public sector organisations (The Public Sector Equality Duty) to integrate consideration of Equality, Diversity and Inclusion into their day-to-day business. The Equality Duty has 3 aims, it requires public bodies to have due regard to the need to:

- **eliminate unlawful discrimination**, harassment, victimisation and other conduct prohibited by the Equality Act of 2010;
- **advance equality of opportunity** between people who share a protected characteristic and people who do not;
- **foster good relations** between people who share a protected characteristic and people who do not.

Equality Impact Assessment (EIA) is a tool for examining the main functions and policies of an organisation to see whether they have the potential to affect people differently. Their purpose is to identify and address existing or potential inequalities, resulting from policy and practice development. Ideally, EIAs should cover all the strands of diversity and Inclusion. It will help us better understand its functions and the way decisions are made by:

- **considering the current situation**
- **deciding the aims and intended outcomes of a function or policy**
- **considering what evidence there is to support the decision and identifying any gaps**
- **ensuring it is an informed decision**

Equality Impact Assessment (EIA) *see supporting guidance on pg 3*

Step 1: Scoping and Identifying the Aims

Service Line / Department	All Employees, Volunteers,	
Title of Change:		
What are you completing this EIA for? (Please select):	Policy	<i>(If other please specify here)</i>
What are the main aims / objectives of the changes	To Provide Guidance to Managers and Employees over the Management of all issues relating to Suspect Packages and Devices. as well as the Protection of Employees, Patients and Visitors from Acts of Unlawful Interference by means of Suspect items and Hoax bomb threats	

Step 2: Assessing the Impact

Please use the drop-down feature to detail any positive or negative impacts of this document /policy on patients in the drop-down box below:

Protected Characteristic	Positive Impact(s)	Negative Impact(s)	Action to address negative impact: <i>(e.g. adjustment to the policy)</i>
Sex			This Policy does not have Negative or positive impact on any protected characteristic such as Sex

Gender reassignment			This Policy does not have Negative of positive impact on any protected characteristic such as Gender Reassignment
Disability			This Policy does not have Negative of positive impact on any protected characteristic such as Disability
Age			This Policy does not have Negative of positive impact on any protected characteristic such as Age
Sexual Orientation			This Policy does not have Negative of positive impact on any protected characteristic such as Sexual Orientation
Pregnancy and maternity			This Policy does not have Negative of positive impact on any protected characteristic such as Pregnancy and Maternity
Marriage and civil partnership			This Policy does not have Negative of positive impact on any protected characteristic such as Marriage and Civil Partnership
Religion or belief			This Policy does not have Negative of positive impact on any protected characteristic such as Religion or Belief
Race			This Policy does not have Negative of positive impact on any protected characteristic such as Race

If you answer yes to any of the following, you MUST complete the evidence column explaining what information you have considered which has led you to reach this decision.

Assessment Questions	Yes / No	Please document evidence / any mitigations
In consideration of your document development, did you consult with others, for example, external organisations, service users, carers or other voluntary sector groups?)	Yes	There has been regular consultation with the H&S manager and Lead for Emergency Planning and Business continuity both areas where this policy falls upon. Regular meetings and updates from the Local Police and Counter terrorism policing specialists
Have you taken into consideration any regulations, professional standards?	Yes	The professional Standards by which the LSMS follows does not impede this policy and or any Impact assessment made as a result of it.
In drafting your document have you identified any discrimination issues, and if so how have they been mitigated?	No	No this policy has no effect on the diversity of people it relates to and also does not discriminate against any one person or organisation based on the protected characteristics. The policy is created to save life and limb in the event an emergency occurs.

Step 3: Review, Risk and Action Plans

How would you rate the overall level of impact / risk to the organisation?	Low	Medium	High
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

What action needs to be taken to reduce or eliminate the negative impact?	N/A no negative impact identified
Who will be responsible for monitoring and regular review of the document / policy?	The Review of this policy and EIA will be conducted by the ASMS or H&S manager

Step 4: Authorisation and sign off

I am satisfied that all available evidence has been accurately assessed for any potential impact on patients and groups with protected characteristics in the scope of this project / change / policy / procedure / practice / activity. Mitigation, where appropriate has been identified and dealt with accordingly.

Equality Assessor:	Date:
--------------------	-------

This section is to be agreed and signed by the Head of Diversity and Inclusion in agreement with the Diversity and Inclusion Strategy Lead:

Diversity and Inclusion authoriser name:	
Date:	

Additional guidance

Protected characteristic	Who to Consider	Example issues to consider	Further guidance
1. Disability	A person has a disability if they have a physical or mental impairment which has a substantial and long term effect on that person’s ability to carry out normal day today activities. Includes mobility, sight, speech and language, mental health, HIV, multiple sclerosis, cancer	<ul style="list-style-type: none"> • Accessibility • Communication formats (visual & auditory) • Reasonable adjustments. • Vulnerable to harassment and hate crime. 	Further guidance can be sought from: Solent Disability Resource Group
2. Sex	A man or woman	<ul style="list-style-type: none"> • Caring responsibilities • Domestic Violence • Equal pay • Under (over) representation 	Further guidance can be sought from: Solent HR Team
3. Race	Refers to an individual or group of people defined by their race, colour, and nationality (including citizenship) ethnic or national origins.	<ul style="list-style-type: none"> • Communication • Language • Cultural traditions • Customs • Harassment and hate crime • “Romany Gypsies and Irish Travellers”, are protected from discrimination under the ‘Race’ protected characteristic 	Further guidance can be sought from: BAME Resource Group
4. Age	Refers to a person belonging to a particular age range of ages (e.g., 18-30 year olds) Equality Act legislation defines age as 18 years and above	<ul style="list-style-type: none"> • Assumptions based on the age range • Capabilities & experience • Access to services technology skills/knowledge 	Further guidance can be sought from: Solent HR Team

5	Gender Reassignment	“ The expression of gender characteristics that are not stereotypically associated with ones sex at birth” World Professional Association Transgender Health 2011	<ul style="list-style-type: none"> • Tran’s people should be accommodated according to their presentation, the way they dress, the name or pronouns that they currently use. 	Further guidance can be sought from: Solent LGBT+ Resource Group
6	Sexual Orientation	Whether a person’s attraction is towards their own sex, the opposite sex or both sexes.	<ul style="list-style-type: none"> • Lifestyle • Family • Partners • Vulnerable to harassment and hate crime 	Further guidance can be sought from: Solent LGBT+ Resource Group
7	Religion and/or belief	Religion has the meaning usually given to it but belief includes religious and philosophical beliefs, including lack of belief (e.g Atheism). Generally, a belief should affect your life choices or the way you live for it to be included in the definition. (Excludes political beliefs)	<ul style="list-style-type: none"> • Disrespect and lack of awareness • Religious significance dates/events • Space for worship or reflection 	Further guidance can be sought from: Solent Multi-Faith Resource Group Solent Chaplain
8	Marriage	Marriage has the same effect in relation to same sex couples as it has in relation to opposite sex couples under English law.	<ul style="list-style-type: none"> • Pensions • Childcare • Flexible working • Adoption leave 	Further guidance can be sought from: Solent HR Team
9	Pregnancy and Maternity	Pregnancy is the condition of being pregnant or expecting a baby. Maternity refers to the period after the birth and is linked to maternity leave in the employment context. In non-work context, protection against maternity discrimination is for 26 weeks after giving birth.	<ul style="list-style-type: none"> • Employment rights during pregnancy and post pregnancy • Treating a woman unfavourably because she is breastfeeding • Childcare responsibilities • Flexibility 	Further guidance can be sought from: Solent HR team