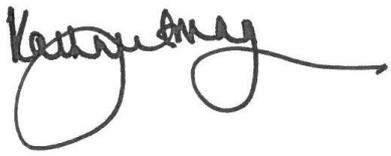


Checklist for the Review and Approval of Procedural Document

To be completed and attached to any document which guides practice when submitted to the appropriate committee for consideration and approval.

	Title of document being reviewed:	Yes/No/ Unsure	Comments
1.	Title	Yes	
	Is the title clear and unambiguous?	Yes	
	Is it clear whether the document is a guideline, policy, protocol or standard?	Yes	
2.	Rationale		
	Are reasons for development of the document stated?	Yes	
3.	Development Process		
	Is the method described in brief?	Yes	
	Are people involved in the development identified?	Yes	
	Do you feel a reasonable attempt has been made to ensure relevant expertise has been used?	Yes	
	Is there evidence of consultation with stakeholders and users?	Yes	
4.	Content		
	Is the objective of the document clear?	Yes	
	Is the target population clear and unambiguous?	Yes	
	Are the intended outcomes described?	Yes	
	Are the statements clear and unambiguous?	Yes	
5.	Evidence Base		
	Is the type of evidence to support the document identified explicitly?	N/A	
	Are key references cited?	Yes	
	Are the references cited in full?	Yes	
	Are supporting documents referenced?	Yes	

	Title of document being reviewed:	Yes/No/Unsure	Comments
6.	Approval		
	Does the document identify which committee/group will approve it?	Yes	
	If appropriate have the staff side committee (or equivalent) approved the document?	N/A	
7.	Dissemination and Implementation		
	Is there an outline/plan to identify how this will be done?	Yes	
	Does the plan include the necessary training/support to ensure compliance?	Yes	
8.	Document Control		
	Does the document identify where it will be held?	Yes	
	Have archiving arrangements for superseded documents been addressed?	Yes	
9.	Process to Monitor Compliance and Effectiveness		
	Are there measurable standards or KPIs to support the monitoring of compliance with and effectiveness of the document?	Yes	General emergency preparedness will be assessed against the NHS England Core EPRR Standards
	Is there a plan to review or audit compliance with the document?	Yes	
10.	Review Date		
	Is the review date identified?	Yes	
	Is the frequency of review identified? If so is it acceptable?	Yes	
11.	Overall Responsibility for the Document		
	Is it clear who will be responsible for co-ordinating the dissemination, implementation and review of the documentation?	Yes	

Individual Approval			
If you are happy to approve this document, please sign and date it and forward to the chair of the committee/group where it will receive final approval.			
Name	Caroline Hall	Date	29 November 2017
Signature			
Committee Approval			
If the committee is happy to approve this document, please sign and date it and forward copies to the person with responsibility for disseminating and implementing the document and the person who is responsible for maintaining the organisation's database of approved documents.			
Name	Kathryn Magson	Date	29 November 2017
Signature			

Acknowledgement: Cambridgeshire and Peterborough Mental Health Partnership NHS Trust

SUSPECT PACKAGE AND SUBSTANCE PLAN

Version Number	1.7
Ratified By	HVCCG Exec Team
Date Ratified	October 2017
Name of Originator/Author	Amanda Yeates
Responsible Director	Chief Finance Officer
Staff Audience	All staff
Date Issued	November 2017
Next Review Date	September 2017

This document is available electronically, in a larger font, or alternative format on request.

DOCUMENT CONTROL

Plan Version	Page	Details of amendment	Date	Author
V1		New plan	Jun 13	AY
V1.1	9	Wording of paragraph 2 amended	Jul 13	AY
V1.2	8	References to mobile phone contact amended	Jul 13	AY
V1.2	9	References to mobile phone contact amended	Jul 13	AY
V1.2	12	30 miles changed to 30 metres	Jul 13	AY
V1.3	15	NHS Herts Senior Manager changed to HVCCG	Aug 13	AY
V1.3	16	Trust Switchboard changed to Charter House	Aug 13	AY
V1.4	ALL	Plan review	Sep 14	AY
V1.5	12	Section 6 updated to include annual exercise	Jun 15	AY
V1.5	13	Section 7 location of plans updated to include memory sticks	Jun 15	AY
V1.5	13	Section 8 link to NHSE Core Standards updated	Jun 15	AY
V1.5	13	Additional associated documents added	Jun 15	AY
V1.6	13	Section 10 related documents updated	Jun 15	AY
V1.7	9– 2	General duties in section 3 updated in line with the latest national guidance	Sep 17	AY
V1.7	12	Definitions updated in line with latest national guidance	Sep 17	AY
V1.7	12-17	Section 5 updated in line with latest national guidance	Sep 17	AY
V1.7	17	References updated	Sep 17	AY
V1.7	18	Associated documents updated	Sep 17	AY
V1.7	19	Checklist in appendix A updated in line with latest national guidance	Sep 17	AY
V1.7	24	New Equality Impact Screening document completed	Sep 17	AY

Contents

Section	Page
1 Introduction	7
2 Purpose	7
3 Duties	7
4 Definitions	11
5 Content	11
5.1 Assessing the Threat	11
5.2 Devices and the Damage They Do	11
5.3 Delivered Items	12
5.4 The Bomb in the Building	13
5.5 Telephone Bomb Threats	13
5.6 Building Searches	13
6 Monitoring	11
7 Education and Training	14
8 Standards and Key Performance Indicators	15
9 References	15
10 Associated Documentation	15
 Appendices	
Appendix A Bomb Threat or Security Alert Checklist	16
6Appendix B Public Health England Suspect Packages and Parcels Algorithm	19
Appendix C Instructions on how to deal with a suspicious item	21

1. Introduction

In recent years the world has had to get to grips with the increase of terrorist crime. There are many groups throughout the world who are capable and prepared to plant devices within the UK. Terrorist attacks, and attacks from extremist campaigners or malicious hoaxers, are designed to intimidate, disrupt, cause economic damage and in some cases will cause injury or death. They are not commonplace in the UK, however, when they occur they will attract a lot of publicity.

2. Purpose

This plan is for HVCCG and is aimed at ensuring all staff have a clear understanding of how to respond to the discovery of a suspect package/powder or the receipt of a security alert, be able to provide the responding emergency services with all the necessary information as well as how to evacuate a building if necessary.

3. General Duties within the Organisation

Members of staff may find themselves involved with a suspect package in many different ways, the most common ways are:

- Receiving a telephone call advising there is a bomb somewhere (it may not be connected with your premises or even your organisation). It may be referred to as an IED or Improvised Explosive Device as this term is now common in use.
- Finding a suspect package
- Discovering an unknown powder or substance

Wherever there is the threat that a bomb or IED has been planted then mobile telephones and radios should not be used. The electronic waves from mobile telephones or handheld radios could, unintentionally, activate a device, therefore neither should be used within 30 metres of a suspect package.

Any member of staff with a direct telephone line, mobile phone, computer or tablet etc could conceivably receive a bomb threat. Staff should, therefore, understand the actions required of them as the potential first response to a threat message. In the event a member of staff receives a call advising them a bomb has been planted they should follow these rules:

- Stay calm and listen carefully
- Try to obtain as much information as possible (see the checklist in appendix A)
- If practical, keep the caller talking and alert a colleague to dial 999
- If displayed on your phone, note the number of the caller, otherwise dial 1471 once the call has ended.
- If the threat is a recorded message write down as much information as possible
- If the threat is received via text message do not reply to, forward or delete the message; note the number of the sender and follow police advice
- Report the call to the Police, the office manager and the Senior Manager On Call (SMOC). This should be done in person or using landline telephones if it

is possible that the SMOC is in the vicinity of the device. The on-call rota is held by the Emergency Planning and Resilience Lead and can be accessed on the N drive. If it is outside of normal office hours, or the SMOC is off-site, they can be contacted on 07881 940243 from a land line telephone

If the threat is delivered face to face:

- Try to remember as many distinguishing characteristics of the threat-maker as possible

If discovered in a written note, letter or as graffiti:

- Treat as police evidence and stop other people touching the item

If the threat is received via email or social media application:

- Do not reply to, forward or delete the message
- Note the sender's email address or username / user ID for social media applications
- Preserve all web log files for your organisation to help the police investigate (as a guide, 7 days prior to the threat message and 48 hours after)

Remember that all records (written, typed or electronic) must be kept and may be required by the police as part of their investigation process.

On receipt of a notification of an incident the SMOC / Director On Call or Chief Executive will decide on the level and type of response required. Where the Emergency Planning and Resilience Lead is available they will assist in the co-ordination of the response, taking the role of lead officer if required to do so by the SMOC. If the Emergency Planning and Resilience Lead is not available a lead officer should be appointed by the SMOC. The decision making process should not be delayed waiting for the arrival of the police. All bomb threats should be reported to the police and their subsequent advice followed accordingly

A suspicious powder incident may only become evident on opening a letter or package. The actions to take upon discovery of a suspicious package are:

- Put the item down on a cleared, flat surface
- Keep it separate so it is clearly identifiable
- Do not move it
- Do not use mobile phones or two way radios in the cleared area or within 30 metres of the suspect package
- Notify the SMOC. The on-call rota is held by the Emergency Planning and Resilience Lead and can be accessed on the shared drive. If it is outside of normal office hours, or the SMOC is off-site, they can be contacted on 07881 940243 from a land line telephone.
- Call the Emergency Planning and Resilience Lead on 01442 284059 from a land line telephone
- Arrange to clear the immediate area and each adjacent room, including rooms above and below
- If there is any suggestion of chemical, biological or radiological materials, move those directly affected to a safe location close to the incident, keep these individuals separate from those not involved

- Prevent others approaching or accessing the cleared areas
- Notify the police. If the item has been opened, or partially opened prior to being deemed suspicious, it is vital that this is communicated to the police.
- Communicate regularly with staff, visitors and the building management team
- Ensure witnesses remain available to brief the police, and the accuracy of their observations is preserved; encourage witnesses immediately to record their observations in writing, and discourage them from discussing the incident or their observations with others prior to the arrival of the police
- If a CBR incident is suspected then undertake improvised decontamination of contaminated individuals as quickly as possible, ideally within the first 15 minutes
- In the event of a CBR incident occurring, lifts should not be used in order to move around or evacuate the building

Any air ventilation systems should be shut. If you have been contaminated or believe you have been, blow your nose and wash your hands thoroughly. Do not touch your eyes, nose, mouth or other parts of your body, Do not eat, drink or smoke.

A Public Health England Action Card is attached in appendix B and laminated copies of this action card and the steps for dealing with an event should be displayed as appropriate.

During an incident the Communications Team must be kept informed at all times in order to ensure the effectiveness of communications to staff as well as the co-ordination of any press/media statements. All media enquiries must be directed to the Communications Team who will be responsible for all media contact.

Following the receipt of a security alert or after finding a suspicious package or powder there may be the need to evacuate a building. Staff should be advised of the need to evacuate in a pre-determined way this should be different to a Fire Evacuation, it maybe by word of mouth giving staff clear instructions as to what is expected of them. Staff should leave via an agreed designated route. This route will avoid the area where the suspicious package is and will be the safest route rather than the quickest route. Designated Fire Marshals should ensure the staff leave the building in the most appropriate manner.

Where it is safe to do so staff should take with them personal possessions such as keys, wallets, handbags and coats as re-entry to the building may be restricted for some time. An assembly area at least 500 meters away from the building should be used, up wind and uphill if possible and where possible car parks should not be used. This will put staff a safe distance away from flying debris caused by the suspect package they have been evacuated away from.

Reoccupation will only take place following detailed discussions between the SMOC and the Police and/or the Military Explosive Ordinance Disposal (EOD) Personnel. Consideration should always be given to there being secondary devices either within the building or near to where staff are going to assemble having left the building.

The Police or other emergency services representative may advise of the necessity to do only a partial evacuation of the building; their advice on which areas are to be evacuated must be followed. Staff within the designated area will be informed of the need to evacuate by word of mouth. Where staff may have, or actually have, come into contact with an unknown substance they may be asked to remain in a secure area, the advice of the police or other appropriate specialist will be followed on this matter.

Where possible, an e-mail will be sent out by the Communications Team or other nominated person detailing the cordoned off areas or assembly points and any contingency arrangements put in place. The Communications Team will be responsible for ensuring staff are kept up to date on the response and on any possible disruptions to services, access to buildings etc. The Communications Team can also co-ordinate any necessary signage.

There are occasions when it is safer to remain inside and move people away from the external windows and walls, e.g. if it is known that a bomb is not within or immediately adjacent to the building. If the suspect device is outside of the office, people may be exposed to greater danger if the evacuation route inadvertently takes them past the device. However, if the location of the threatened device is unknown, evacuation presents a credible and justifiable course of action.

A decision not to outwardly or inwardly evacuate will be reasonable and proportionate if, after an evaluation by the SMOC / DoC or Chief Executive, the threat is deemed implausible (e.g. a deliberate hoax). In such circumstances police may provide additional advice and guidance relating to other risk management options. It may be considered desirable to ask staff familiar with the venue to check their immediate surroundings to identify anything out of place.

The all clear will be declared by the SMOC or other nominated Director or in their absence by the Emergency Planning and Resilience Lead. It will only be declared on agreement with the police officer in charge. On receipt of this agreement the appointed Lead Officer will be responsible for co-ordinating the return to normal. The Communications Team or other nominated person will be responsible for cascading this message to all staff.

The appointed Lead Officer will ensure that if required the police and emergency services have a future point of contact for their investigations. The Emergency Planning and Resilience Lead will co-ordinate the preparation of any reports and the safe keeping of all documents relating to the incident and response. Such information and reports may be required by the police as part of their investigation process.

4. Definitions

CBR – Chemical, Biological, Radiological
EOD – Explosive Ordnance Disposal
HVCCG – Herts Valleys Clinical Commissioning Group
IED – Improvised Explosive Device
PBIED – Person Borne IED
RCIED – Radio Controlled IED
SMOC – Senior Manager On Call
UVIED – Under Vehicle IED
VBIED – Vehicle Borne IED
VOIED – Victim Operated IED

5. Content

5.1 Assessing the threat

Evaluating the credibility of threat is a critical task, particularly if the attack being threatened is imminent. Police will assess the threat at the earliest possible opportunity. However, in the absence of detailed information it will be necessary to consider a number of factors:

- Is the threat part of a series? If so, what has happened elsewhere or previously?
- Can the location of the claimed bomb(s) be known with precision? If so, is a bomb visible at the location identified?
- Considering the hoaxer's desire to influence behaviour, is there any reason to believe their words?
- If the threat is imprecise, could an external evacuation inadvertently move people closer to the hazard?
- Is a suspicious device visible?

Any level of threat should be assessed on an ongoing basis, the risk to an individual organisation or set of premises will change depending on the activities going on in the community or the world.

It is believed that the health economy is at a very low risk of receiving suspect packages from known terrorist organisations, however, the risk from lone crusaders (also known as "lone wolf" terrorists) or people with a grudge can never be under estimated.

5.2 Devices and the Damage They Do

An Improvised Explosive Device (IED) is a "home made" bomb. The main explosive charge in an IED may be made from home made explosive (HME) and may be still as powerful as commercial or military explosives. Although an IED is "home made," it can be highly sophisticated and very effective.

They can be delivered using the following methods:

- Radio controlled IED (RCIED) initiated electronically via a wireless method consisting of a transmitter and receiver (i.e. mobile phone, pager etc)
- Person Borne Improvised Explosive Device IED (PBIED)

- Postal device (delivered) – often a Victim Operated IED (VOIED)
- Vehicle Borne IED (VBIED) – a vehicle that contains and delivers an explosive device to a target
- Under vehicle IED (UVIED) – small explosive devices typically attached to or placed underneath a vehicle
- Time bomb IED – IED initiated by a timer switch
-

It is believed the most likely attack, if it was to happen, would be via explosive or incendiary items which are delivered by post or hand.

5.3 Delivered Items

Delivered items, which include malicious letters, parcels, packages and anything delivered by post or courier, have been a commonly used tactic by criminals and terrorists. Delivered items may be explosive, incendiary or contain sharp blades, or chemical, biological or radiological (CBR) material. The phrase “white powders” is often used in the context of main and encompasses CBR material as well as benign materials (note: such materials may not be white and may not be powders). Anyone receiving a suspicious delivery is unlikely to know which type it is.

A delivered item may have received some rough handling in the post and so is unlikely to detonate through being moved. Any attempt at opening it, may set off or release the contents. Threat items come in a variety of shapes and sizes; a well-made device will look innocuous but there may be tell-tale signs.

General indicators that a delivered item may be of concern include:

- An unexpected item, especially of hand delivered
- A padded envelope or other bulky package
- An additional inner envelope or other contents that may be difficult to remove
- Labelling or excessive sealing that encourages opening at a particular end or in a particular way
- An item that is oddly shaped or lopsided
- An envelope flap stuck down completely (normally gummed envelope flaps leave slight gaps at edges)
- An item marked “to be opened by...”, “personal” or “confidential.”
- An item addressed to the organisation or a title (rather than a specific individual).
- An unexpected or unusual origin (postmark and / or return address)
- No return address or a return address that cannot be verified
- An item that is poorly or inaccurately addressed, address printed unevenly or unusually
- Unfamiliar writing or unusual style
- An unusual postmark or no postmark
- More stamps than are needed for the size or weight of the package
- Greasy or oily stains emanating from the package
- Odours emanating from the package

Explosive or incendiary indicators include:

- Unusually heavy or uneven weight distribution
- Small hole(s) in envelope or wrapping

“White powder” indicators include:

- Powders, liquids emanating from the package
- Wrapping stained by liquid leakage
- Unexpected items or materials found in package on opening (loose in a container) such as powdered, crystalline or granular solids; liquids; sticky substances or residues
- Unexpected odours observed on opening
- Sudden onset of illness or irritation of skin, eyes and nose

5.4 The Bomb in the Building

One threat to be aware of is the leaving of hand-carried devices (such as holdalls) in public places to which access is simple. A device of this size can kill or maim anyone close to the seat of the blast, inflict injury on people as well as causing general damage to the structure of the building, in particular the glazing.

5.5 Bomb Threats

A bomb threat can be communicated in a number of different ways. The threat is likely to be made in person over the telephone; however, it may also be a recorded message, communicated in written form, delivered face-to-face or, increasingly, sent by email or social media (e.g. twitter or facebook etc). A threat may be communicated via a third party, i.e. a person or organisation unrelated to the intended victim and identified only to pass the message.

Bomb threats containing accurate and precise information, and received well in advance of an actual attack, are rare occurrences. The vast majority of cases are hoaxes, and the intent is social engineering, to cause disruption, fear and inconvenience.

5.6 Building Searches

If a bomb threat is received, it may be decided to initiate a search for suspicious items. Fire Marshalls and Deputy Fire Marshalls will be responsible for searching their allocated areas of the office in line with the agreed “search” plan and without alarming other staff or visitors. The search will be coordinated by the Tenant Incident Controller.

Bombs and incendiary devices are disguised in many ways. Searchers do not have to be expert in explosive devices. They are looking for anything that

- Should not be there
- Cannot be accounted for
- Is out of place

When looking for a suspect package, mobile telephones must be switched off. Under no circumstances should any suspicious items be touched or moved in any way. Apply the 4 C's protocol: **Confirm, Clear, Communicate and Control**.

Confirm whether or not the item exhibits recognisably suspicious characteristics:

- Is it hidden? Has the item been deliberately concealed or is it obviously hidden from view?
- Is it obviously suspicious? Does it have wires, circuit boards, batteries, tape, liquids or putty like substances visible? Could it pose an immediate threat to life?

Is the item typical of what you would expect to find in this location? Most lost property is found in locations where people congregate, Check if anyone has left the item. If the item is assessed to be unattended, rather than suspicious, examine further before handing to the Corporate Support team as lost property.

If the item is classed as suspicious, **clear** the immediate area:

- The item should not be touched
- People should be moved away to a safe distance. Even for a small item, such as a briefcase, move at least 100m away from the item starting from the centre and moving out
- People should remain out of the line of sight of the suspicious item as if the item cannot be seen, the better protected you will be.
- People should hide behind something substantial if possible, away from glass such as windows and skylights,
- The area should be cordoned off.

Communicate by calling 999. Inform the SMOC.

Control access to the cordoned area. Staff and visitors should not be able to approach the area until it is deemed safe. Eyewitnesses should remain on hand so that they can tell the police what they saw.

Mobile phones and radios should not be used within a 30 metre radius of the suspect package, and if used beyond this point should only be used behind a hard cover.

6. Monitoring

The effectiveness and efficiency of and compliance with the overall Emergency Planning and Resilience programme, will be assured by:

- Annual review of the appropriateness of all emergency planning and resilience policies, their objectives and scope, in line with the most up to date local and national guidance
- Annual renewal of all Emergency and Business Continuity Plans
- Annual exercise of the plan as appropriate

This is the responsibility of the Emergency Planning and Resilience Lead, who is also responsible for the appropriate distribution of this plan.

7. Education and Training

It is the responsibility of Directors and Managers to ensure that they and their teams are aware and understand their roles and responsibilities in the event of a business disruption and/or emergency situation. All Herts Valleys Clinical Commissioning Group staff should be aware of this policy. An electronic copy of the policy is available in the Resource Centre of HVCCG's website under "Policies and Guidance Documents." All emergency planning policies are also held on memory sticks located in the "battle box" in Apsley Room, with the Emergency Planning and Resilience Lead, Chief Executive and Chief Finance Officer.

8. Standards/Key Performance Indicator

HVCCG performance against general Emergency Preparedness, Resilience and Response will be measured against the NHS England Core Standards for Emergency Preparedness, Resilience and Response

9. References

- Public Health England Suspect Packages (white powder incidents) Algorithm v 2.2 November 2006
- Multi-Agency Arrangements for Responding to a Chemical, Biological, Radiological, Nuclear or Explosive (CBRNE) Incident v6.4 (July 2017)
- NaCTSO Crowded Places Guidance 2017

10. Associated Documents

- NHS Hertfordshire Suspect Package and Substance Plan June 2012
- HVCCG CBRN plan October 2017
- HVCCG Incident Plan October 2017
- HVCCG Business Continuity Plan October 2017
- HVCCG Incident Co-ordination Centre plan October 2017

BOMB THREAT OR SECURITY ALERT CHECKLIST

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 had 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

- **ASK THESE QUESTIONS AND RECORD ANSWERS AS ACCURATELY AS POSSIBLE**

1. Where 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 COMPLETED.....

- **INFORM SMOC (07881 940243) and the Emergency Planning & Resilience Lead 01442 284059)**

– Name person(s) informed.....

DIAL 999 AND INFORM POLICE – Time informed.....

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

Date and time of call.....

Duration of the call.....

The telephone number that received the call

ABOUT THE CALLER

Male Female Approximate age.......

Nationality.....

THREAT LANGUAGE

Well-spoken Irrational Taped Foul Incoherent

Message read from text by threat maker

CALLERS VOICE

Calm Crying Clearing throat Angry Nasal Slurred

Excited Stutter Disguised Slow Lisp Accent*

Rapid Deep Hoarse Laugh Familia

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

What accent?.....

OTHER SOUNDS

Street noises House noises Animal noises Crockery PA system

Clear Booth Factory machinery Office machinery Static

Voice Music Motor Other

Remarks

Additional notes

Signature:.....

Print name.....

Date.....

**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 organisation 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 OR
COORDINATING MANAGER**

Retention period: 7 years

Appendix B

Public Health England Suspect packages and parcels algorithm

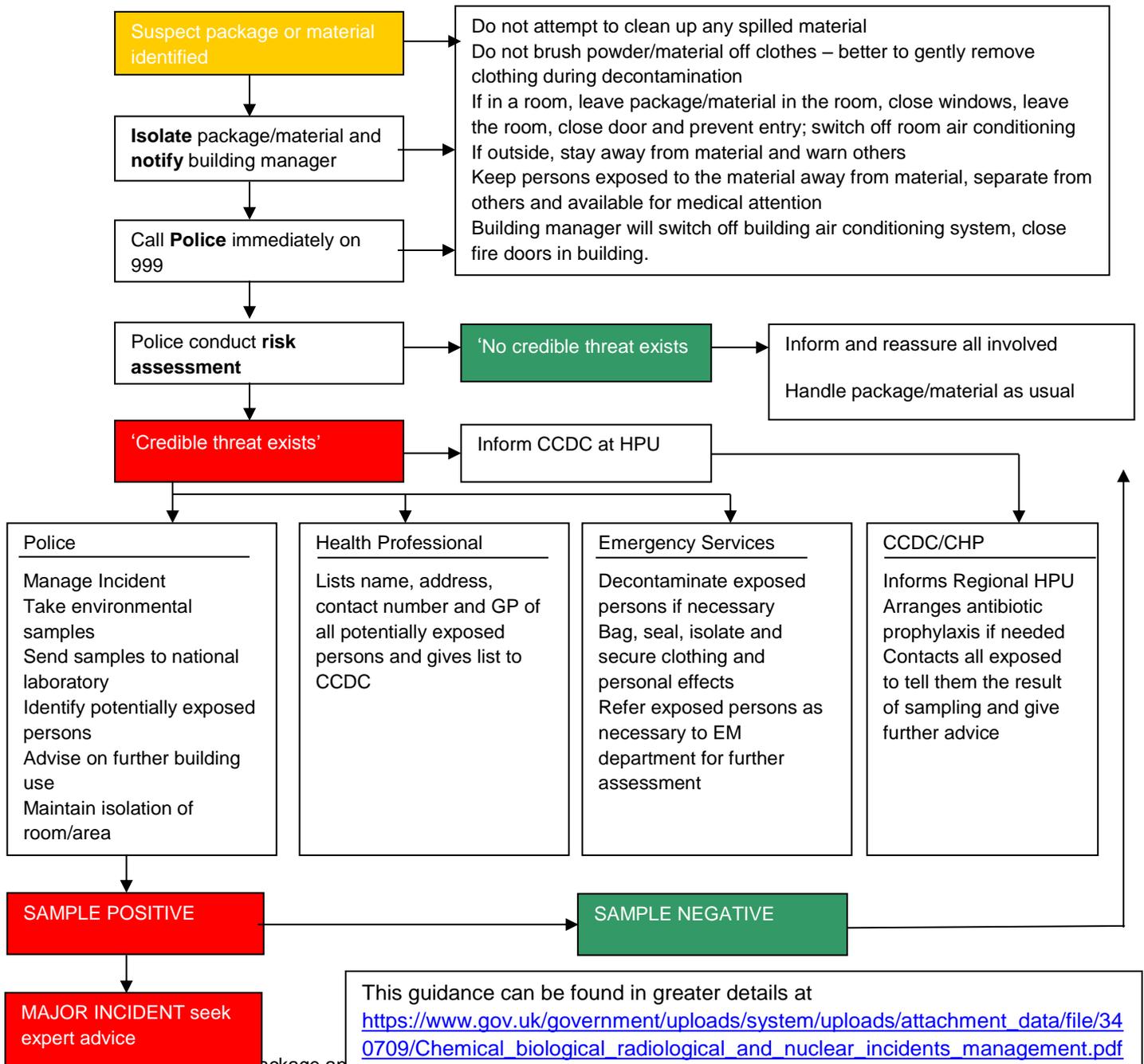
Remember

If you are EVER in ANY doubt about a package, letter or parcel
DO NOT OPEN IT, HANDLE IT, OR MOVE IT, CALL THE POLICE ON 999

Signs that might trigger suspicion include

- Any envelope or package with a suspicious or threatening message written on it or contained inside
- Oily stains, strange odours
- Envelopes that are lopsided, rigid, bulky, discoloured, or feel as though they contain powder
- Unexpected envelopes or packages from foreign countries
- No postage stamp, no franking, no cancellation of the postage stamp, excessive postage
- Incorrect spelling of common names, places or titles
- Handwritten envelopes/packages from an unknown source particularly if addressed to an individual and marked 'personal' or 'addressee only'
- Symptoms (runny nose, streaming eyes, cough, skin irritation) in exposed persons

Suspect package management algorithm



DEALING WITH A SUSPICIOUS ITEM – STEPS TO BE TAKEN

If you have detected a suspicious item:

- **Leave it alone – do not touch or try to move it**
- **Clear and secure the immediate area making sure everyone is accounted for**
- **Segregate those who may be directly contaminated**
- **Ensure that the police will still have unhindered access to the suspicious item**
- **Call the Police using 999 – wherever there is the threat of a bomb mobile phones should not be used**
- **Use a land line telephone and NOT a mobile**
- **Notify the Senior Manager On Call 07881 940243**
- **Notify the Emergency Planning and Resilience Lead 01442 284059**

APPENDIX D - HVCCG Equality Impact Assessment Screening Form

Very occasionally it will be clear that some proposals will not impact on the protected equality groups and health inequalities groups.

Where you can show that there is no impact, positive or negative, on any of the groups please complete this form and include it with any reports/papers used to make a decision on the proposal.

Name of policy / service	Suspect package and Substance plan
What is it that is being proposed?	<p>Members of staff may find themselves involved with a suspect package in many different ways, the most common ways are:</p> <ul style="list-style-type: none"> •Receiving a telephone call advising there is a bomb somewhere (it may not be connected with your premises or even your organisation). It may be referred to as an IED or Improvised Explosive Device as this term is now common in use. •Finding a suspect package •Discovering an unknown powder or substance
What are the intended outcome(s) of the proposal	<p>This plan is for HVCCG and is aimed at ensuring all staff have a clear understanding of how to respond to the discovery of a suspect package/powder or the receipt of a security alert, be able to provide the responding emergency services with all the necessary information as well as how to evacuate a building if necessary.</p>
Explain why you think a full Equality Impact Assessment is not needed	<p>This policy will not assist with any of the aims of the Equality Act or have any specific impact on the characteristic groups</p>
On what evidence/information have you based your	<p>The contents of the policy</p>

decision?	
How will you monitor the impact of policy or service?	Please see section 5 of the policy "Monitoring Compliance"
How will you report your findings?	Via annual audit against the NHSE Core Standards for EPRR

Having considered the proposal and sufficient evidence to reach a reasonable decision on actual and/or likely current and/or future impact I have decided that a full Equality Impact Assessment is not required.	
Assessors Name and Job title	Amanda Yeates
Date	September 2017