NHS
Leeds West
Clinical Commissioning Group

NHS LEEDS WEST CCG
SECURITY POLICY & PROCEDURE

Last Review Date Approving Body Date of Approval Date of Implementation Next Review Date Version	N/A Audit Committee 8 March 2017 8 March 2017 March 2020 1.0
Related Policies / Procedures	Lone Working Procedure Acceptable Standards of Behaviours Policy Managing Violence, Abuse and Aggression Procedure

CONTENTS

DEFINITIONS

Term **Definition**

Counter Fraud and Security Management Service (CFSMS)

The NHS Counter Fraud Service was established in 1998 as a specialist organisation with the commitment to protect the NHS by ensuring that resources made available to patient care and services are not lost to fraud and corruption. The much larger CFSMS was officially inaugurated as a Special Health Authority on 1 April 2003. Since 1 April 2006 it has been a division of the NHS Business Services Authority, and operating as NHS Protect. It is strategically placed with its operational and policy roles to effectively counter fraud and, with a wide remit to manage healthcare security arrangements within the NHS.

Local Security Management Specialist (LSMS)

The Local Security Management Specialist (LSMS) is highly trained by NHS Protect and will be involved in performing a wide range of security-related tasks:

- Creating a ‘pro-security’ culture amongst staff, professionals and the public
- Deterring those who may be minded to breach security
- Preventing security incidents or breaches from occurring
- Detecting security incidents and reporting them to the CFSMS
- Investigating security incidents in a fair, objective and professional manner
- Applying a wide range of sanctions against those responsible for security incidents, involving a combination of procedural, disciplinary, civil and criminal action as appropriate
- Seeking redress through the criminal and civil justice systems against those whose actions lead to loss of NHS resources
- To deter Criminal activities where possible by putting in place essential security control systems and other counter measures
- To deny the criminal opportunity, not only through physical barriers, but by putting in place effective systems of loss prevention and property control
- To detect the criminal act. The earlier the criminal act is detected and reported the greater the chances of preventing the offenders getting away. Raised awareness of security at all levels will both detect and reduce the risk of crime
- To respond effectively to security issues and problems

Term **Definition**

with workable counter measures

- To review the strategy after every incident, also after counter measures have been put in place to evaluate their effectiveness
- To liaise with the local police and the local authority to achieve partnership working towards a safe and secure environment

The Local Security Management Specialist will work closely with the local Counter Fraud Services Officer to prevent and detect crime and fraudulent activities.

Property

Can be defined as the physical buildings in which NHS staff and professionals work, where patients are treated and from where the business of the NHS is delivered. Ref: *A Professional Approach to Managing Security in the NHS, NHS Counter Fraud and Security Management Service (2003)* http://www.nhsbsa.nhs.uk/Documents/sms_strategy.pdf

Assets

Assets, irrespective of their value can be defined as the materials and equipment used to deliver NHS healthcare. In respect of staff, professionals and patients, it can also mean the personal possessions they retain whilst working in, using or providing services to the NHS. *A Professional Approach to Managing Security in the NHS, NHS Counter Fraud and Security Management Service (2003)* http://www.nhsbsa.nhs.uk/Documents/sms_strategy.pdf

Premises

Premises are land and buildings together considered as a property.

SECTION A – POLICY

1. Policy Statement, Aims & Objectives

1.1 NHS Leeds West Clinical Commissioning Group (CCG) is committed to a safe and secure environment that protects staff, patients and visitors, and their property and the physical assets of the CCG, via Health and Safety legislation, by Department of Health Policy and by common law duty of care. This policy aims to deal proactively with the CCG's security arrangements.

1.2 The CCG will endeavour to ensure necessary resources are made available to fulfil the policy requirements.

1.3 The CCG acknowledges its responsibility to monitor the implementation and progress of this policy and to review on a regular basis. Assurance will be gained on the effectiveness of these measures by independent review and assessments, e.g. NHS Protect initiatives.

1.4 The aim is of this policy is to ensure that wherever possible effective measures are taken to:

- Protect the safety, security and welfare of staff, patients and the general public whilst on CCG premises.
- Provide systems and safeguards against crime, loss, damage or theft of property and equipment.
- Minimise disruption or loss of service to patients/clients.

1.5 It is the CCG's intention to take all reasonable practicable steps to reduce the associated risks from security issues.

1.6 The CCG will ensure, so far as is reasonably practical, that all employees who are required to work alone for significant periods of time are protected from risks to their health and safety.

1.7 The CCG will ensure it has arrangements in place to meet the requirements of the NHS Protect Security Management Standards for Commissioners. The CCG will determine its level of compliance through the completion of a self-review tool (SRT). This is an annual requirement and will be returned to NHS Protect by the specified deadline. The SRT covers the key area of activity outlined in the standards and will be used to inform the development of an ongoing review of the annual work plan by the LSMS in conjunction with the Chief Finance Officer.

2. Legislation & Guidance

2.1. The following legislation and guidance has been taken into consideration in the development of this procedural document:

- The Private Security Industry Act 2001

- The Regulation of Investigatory Powers Act 2000
- Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (RIDDOR) 2013 as amended
- Data Protection Act 1998
- The Protection from Harassment Act 1997
- Control of Substances Hazardous to Health 2004 Approved Codes of Practice
- The Health and Safety at Work Act 1974
- Human Rights Act 1998
- Criminal Procedure and Investigation Act 1996
- Police and Criminal Evidence Act 1984
- Criminal Justice and Public Order Act 1994
- CCTV Code of Practice 2000
- Standards for Commissioners issued by NHS Protect

3. Scope

3.1. This policy applies to those members of staff that are directly employed by NHS Leeds West CCG and for whom the CCG has legal responsibility. For those staff covered by a letter of authority / honorary contract or work experience this policy is applicable whilst undertaking duties on behalf of NHS Leeds West CCG or working on NHS Leeds West CCG premises and forms part of their arrangements with the CCG. As part of good employment practice, agency workers are also required to abide by NHS Leeds West CCG policies and procedures, as appropriate, to ensure their health, safety and welfare whilst undertaking work for the CCG.

4. Accountabilities & Responsibilities

4.1 Security is a management responsibility and the provision of a security service in no way relieves management at any level of its obligations to fulfill the stated purpose of security in the CCG. Managers are required not only to exercise preventative aspects but also to take appropriate action where necessary in respect of those who offend against the law, commit misconduct or other breach of security in contravention of the policies of the CCG.

4.2 The overall accountability for ensuring there are systems and processes to effectively manage security lies with the Chief Finance Officer. They take risks to the CCG from breaches of security seriously and will seek to reduce the numbers of incidents occurring. Responsibility for security is also delegated to the following individuals:

Chief Finance Officer	The Chief Finance Officer functions as the Security Management Director and has lead responsibility for the development and strategic review of security within the CCG, in line with National Guidance including Secretary of State's Directions of November 2003 and NHS Protect Standards for

	Commissioners. The Security Management Director is responsible for: • The formulation, implementation and maintenance of an effective Security Policy (following NHS Protect guidance) in consultation with staff representatives, and ensuring that managers co-ordinate and implement the Policy in their respective areas. • Reviewing and amending this policy to ensure compliance with any current guidance. • Instituting regular campaigns to highlight the importance of security and the responsibilities of all CCG staff. • Leading Security Management within the CCG and identifying security initiatives for improving the security across the CCG. • Advising the CCG of any requirements, statutory or other, by the preparation of procedures for dealing with crime prevention, supply of security systems and maintenance. • Monitoring the performance of the CCG with regard to the implementation of this policy.
Local Security Management Specialist (LSMS)	The nominated Local Security Management Specialist (LSMS) is provided by Audit Yorkshire. The overall objective of the LSMS will be to work on behalf of the CCG to deliver an environment that is safe and secure. This objective will be achieved by working in close partnership with stakeholders within the CCG, NHS Protect and external organisations such as the police, professional representative bodies and trade unions. The LSMS will aim to provide comprehensive, inclusive and professional security management services for the CCG and work towards the creation of a pro-security culture within the NHS. The LSMS will: • Report to the Chief Finance Officer (Security Management Director (SMD)) on security management work locally. • Lead on the day to day work within the CCG to tackle violence against staff and professionals in accordance with national guidance. • Ensure that lessons are learned from security incidents, and that these incidents are assessed and the impact on the CCG reported to appropriate authorities in accordance with guidelines issued by the NHS SMS. • Investigate security incidents/breaches in a fair, objective and professional manner so that the appropriate sanctions and preventative action can be taken • Ensure that the security management policy addresses all the organisations identified risks and contains all the

	required elements from NHS Protect guidance. • Ensure that the security management policy is reviewed or evaluated to establish its effectiveness. • Ensure that any corrective or preventative actions identified as a result of the policy review or evaluation are implemented, to ensure that the security management policy continues to address the CCG's identified risks. • Assist line / senior managers with completion of risk assessments • Produce an annual activity work plan aligned to the resource made available
Other Senior Managers and Head of Service	Other Senior Managers and Head of Service, on behalf of the Chief Officer are responsible for ensuring that the CCG's Security Policy is implemented within the organisation. This will include responsibility for: • Planning any capital investment required to address matters arising from risk assessments. • Security risk assessment within their areas and for ensuring that staff for whom they are responsible are aware of these risks. • Preventative measures and appropriate action in respect of persons who are suspected of committing a criminal offence, misconduct or other breach of security in contravention of the policies of the CCG. • Ensuring staff awareness of and how to access this policy and other relevant documents and their responsibilities and also ensure that staff (including temporary staff) receive training appropriate to the risks involved. • Ensuring that security arrangements within their area are being observed and that deficiencies are reported. • Ensuring that any particular security problems known to them are reported accordingly. • Actively reviewing the security arrangements within their area by carrying out routine audits themselves with the co-operation of staff organisations, in line with CCG risk assessment procedures. • Ensuring that every member of staff obtains a security ID badge and that the badge is worn and visible at all times whilst the staff member is on CCG premises or on CCG business. • An ongoing commitment to staff training, carrying out risk assessments, identifying areas at greatest risk and eliminating or controlling these risks.
Line Managers	Line Managers are responsible for: • Ensuring compliance with CCG Security Policy requirements in the areas for which they are responsible. • The completion of any risk assessments required in

	relation to security of staff or premises. • Ensuring that any security problems known to them are reported accordingly
Staff	Responsibilities of Staff (including all employees, whether full/part time, agency, bank or volunteers) are: • To co-operate with management to achieve the aims and objectives of the Security Policy. Great emphasis is placed on the importance of co-operation of all staff in observing security and combating crime. • The protection and safe keeping of their private property. Any loss of private property must be reported without delay. If private property has been stolen, then it is the owner's responsibility, not the CCG's responsibility to contact the Police. • To familiarise themselves with o any special security requirements relating to their place of work or work practices o the action to take in the event of a security incident • To safeguard themselves, colleagues, visitors, patients/clients etc., so far as is reasonably practicable, and ensure that neither equipment nor property are put in jeopardy by their actions or omissions, either by instruction, example or behaviour. • To follow prescribed working methods and security procedures at all times. • To co-operate with managers to achieve the aims of the Security Policy. • To comply with all training requirements concerning security issues. • To ensure that the CCG ID is worn and visible whenever on CCG premises or on CCG business. • To notify their line manager of any potential security problems and report all incidents involving criminal activity to the appropriate manager. ▪ To report any crime/breach of security. This procedure is documented as Appendix 1. All staff are reminded that wilful failure to carry out responsibilities may result in disciplinary proceedings in accordance with the CCG's Disciplinary Policy. All staff are reminded that it is an offence to remove property belonging to the CCG without written authority. Failure to seek authority from their line manager could result in disciplinary action or criminal proceedings being taken. NHS Leeds West CCG will not accept liability for the loss of, or damage to private property including motor vehicles or

	other modes of transport. Motor vehicles are brought onto the sites entirely at the owner's risk. The CCG will take reasonable steps to safeguard vehicles on their property.

5. Dissemination, Training & Review

5.1. Dissemination

5.1. The Security Policy is located on the CCG's website. Staff are notified by email of new or updated procedural documents.

5.2. Training

5.2.1 The CCG will ensure that appropriate information, instruction and training is given to employees who may be required to work alone, to ensure that so far as is reasonably practicable a safe system of work is in operation. Training will include physical security of assets and premises, and personal safety of staff.

5.2.5 Frontline Staff need to undergo Conflict Resolution Training and attend refresher training on a 3 yearly basis, as well as preventing and reporting crime in the workplace. This mandatory training must be included in departmental programmes as part of in-service training, and with periodic refresher courses. Training involves dealing with situations of potential or actual abuse, aggression of violence, and includes:

- understanding the causes;
- recognising the warning signs;
- identifying when and where to get help;
- interpersonal skills/defusing techniques'

5.3. Review

5.3.1. As part of its development, this procedural document and its impact on staff, patients and the public has been reviewed in line with NHS Leeds West CCG's Equality Duties. The purpose of the assessment is to identify and if possible remove any disproportionate adverse impact on employees, patients and the public on the grounds of the protected characteristics under the Equality Act.

5.3.2. The procedural document will be reviewed every three years, and in accordance with the following on an as and when required basis:

- Legislatives changes
- Good practice guidelines
- Case Law
- Significant incidents reported

- New vulnerabilities identified
- Changes to organisational infrastructure
- Changes in practice

SECTION B - PROCEDURE

1.0 Employment

1.1 All persons applying for a post within the CCG must have completed the section on the application form entitled Rehabilitation of Offenders Act 1974. This section states that ‘because of the nature of the work for which you are applying, this post is exempt from provisions of Section 4(2) of the Rehabilitation of Offenders Act, 1974 (Exemption) Order, 1975.’ Applicants are therefore, not entitled to withhold information about convictions which are ‘spent’ under the provisions of the Act, and in the event of employment, any failure to disclose such convictions could result in dismissal or disciplinary action by the CCG.

1.2 This application form also requests details of any convictions, adult cautions or bind-overs, and requires the applicant to sign the statement confirming that the information given is correct. For more information refer to the Recruitment & Selection Policy.

1.3. In accordance with the provisions of the Children’s Act 1989, the CCG must ensure that, staff who occupy certain positions that brings them regularly in contact with children have a Disclosure & Barring Service check which will be requested as appropriate following appointment of the staff member by the Human Resources Department.

2.0 Personal Security

2.1 Specific procedures for local needs such as domiciliary visits (e.g. lone workers), staff in other premises, reception staff, agile workers etc. are to be developed and implemented by individual departments. All staff must follow existing Health and Safety policies and guidelines.

3.0 Staff Identification

3.1 Every employee, including temporary staff, will be issued with an identification badge on commencement of employment which must be worn at all times whilst on CCG premises or on official business.

3.2 Each member of staff is personally responsible for their badge, and to ensure that the badge is up to date and that there are no radical changes in physical appearance, title or department. All staff should wear an official CCG identification badge and it is the responsibility of each departmental manager to ensure that this is implemented. The identity badge will state the employee name and job title and must be clearly visible to other staff, and visitors.

3.3 Identification badges must be returned to the Office Manager when a member of staff leaves the employment of the CCG. It is the responsibility of the line manager to recover the identity badge from the member of staff concerned and return it to the Office Manager.

3.4 External visitors / contractors should be escorted on site. The member of staff who is responsible for the visitor / contractor must notify the reception staff they are expecting a visitor, provide reception with a contact number so they can be notified of their arrival and arrange for the contractor to be escorted to the relevant department.

4.0 Cash Movement/Handling

4.1 Each Department must ensure that they have suitable and effective procedures in place for the movement of cash/valuables around the CCG. The procedures must take into account the security of the staff as well as the security of the cash/valuables. An example of cash which may be held would be funds raised for charity.

5.0 Funding

5.1 Each Department must take into account security issues including cost implications when:

- Developing schemes for minor improvements
- Developing schemes for new premises, major upgrading etc
- Introducing new services or changes to existing services, which may have implications for staff security.

6.0 Access and Egress

6.1 Access to NHS Leeds West CCG premises is restricted via the use of electronic fobs.

6.2 Every employee will be issued with a fob on commencement of employment. Agency staff, contractors etc. will be issued with a time limited access code to access the premises.

6.3 Each member of staff is personally responsible for their fob and must report any losses to the Office Manager so the fob can immediately be de-activated.

6.4 Fobs must be returned to the Office Manager when a member of staff leaves the employment of the CCG. It is the responsibility of the line manager to recover the fob from the member of staff concerned and return it to the Office Manager.

6.5 External visitors should be escorted on site. The member of staff who is responsible for the contractor / visitor will arrange for the visitor to be escorted to the relevant department.

7.0 Security of Goods

7.1 Goods received into the organisation must be checked against delivery notes prior to signing for acceptance. The organisation will provide secure accommodation for goods awaiting distribution.

7.2 Some CCG goods are received by the landlord and other organisations. These goods will remain the responsibility of the receiving organisation until signed for by a CCG staff member.

7.3 All CCG departments receiving goods must ensure there are procedures in place to monitor the receipt of goods and safe /secure systems are in place to protect goods from theft or inappropriate use.

8.0 Security of Personal Belongings

8.1 All staff should ensure that personal belongings are stored in a secure location e.g. locked in cupboards, lockers or desk drawers. The CCG cannot be held responsible for theft of personal items. The CCG cannot accept liability for loss or damage to staff property.

9.0 Fraud

9.1 The responsibilities for fraud prevention are described in the CCG extranet pages. The Local Security Management Specialist will liaise regularly with the Local Counter Fraud Specialist to ensure a direct and close relationship is maintained.

10.0 Fire

10.1 The overlapping interests of security and fire safety policies are fully recognised and there is full co-operation between fire and security staff.

11.0 Information Security

11.1 Information security risk is inherent in all administrative and business activities and everyone working for or on behalf of NHS Leeds West CCG continuously manages information security risk. The aim of information security risk management is not to eliminate risk, but rather to provide the structural means to identify prioritise and manage the risks involved in all our organisational activities. It requires a balance between the cost of managing and treating information security risks with the anticipated benefits that will be derived.

11.2 All information is held in accordance with the CCG’s Information Governance Policies and associated procedures.

12.0 Violence and Aggression

12.1 The CCG has a duty to provide a safe and secure environment for all employees and visitors and has a zero tolerance approach to violence or abusive behaviour.

12.2 The CCG takes a very serious view of violence, abuse and aggression at work and recognises its responsibility to protect employees and others who may be subjected to any acts of violence, abuse or aggression whether or not the act results in physical or non-physical assault.

12.3 Any member of the public, patients or otherwise who are violent towards CCG staff may have sanctions taken against them, be refused treatment, or taken to court by the CCG in line with NHS Protect Guidance.

13.0 CCTV

13.1 External CCTV is in place on CCG premises. This is managed by the landlord who owns the building and the CCTV system. Requests for access to CCTV images must be made to NHS Property Services (landlord).

14.0 Emergency Preparedness, Resilience & Response

14.1 A significant incident or emergency can be described as any event that cannot be managed within routine service arrangements. Each requires the implementation of special procedures and may involve one or more of the emergency services, the wider NHS or a local authority. Please refer to the Emergency Preparedness, Resilience & Response Plan and Business Continuity Plan.

15.0 Risk Assessment

15.1 The Management (Health, Safety and Welfare) Regulations 1999 (Regulation 3) require that suitable and sufficient risk assessments be undertaken, so that the significance of a hazard can be identified assessed and controlled. Guidance on Assessing risks to safety and health can be found in the CCG's guidance document – Risk Management Strategy.

15.2 Risks associated with security should be reported to the Local Security Management Specialist (LSMS).

15.3 Risk Assessments should be completed for all security hazards including physical (buildings, equipment etc) and people. These risk assessments are the responsibility of the department involved, with support from the Local Security Management Specialist (LSMS) where required.

15.4 Risks relating to security are identified on an ongoing basis through incident reports, complaints and claims procedures, and the risk assessment procedure.

15.5 It is important that all staff within the CCG are aware of the security risks involved within their work. They must also be aware of formal risk assessments that apply to them, the actions identified to control the risks and the measures to be taken by them personally to reduce the risks to themselves and others.

16.0 Lone Working

16.1 When working arrangements are agreed with an individual which result in that person working alone for regular/significant periods, then the manager will be responsible for ensuring that a risk assessment is undertaken and that a related safe system of work is put in place. This will take into account the capability of the individual. The employee will be required to conform to these arrangements, to safeguard both themselves and the CCG.

16.2 Working alone is not illegal, but it can bring additional risks to a work activity. The CCG has developed policies and procedures to control the risks and protect employees, and employees should know and follow them. Apart from the employee being capable of undertaking the work required the three most important aspects to be certain of are that:

- The lone worker has full knowledge of the hazards and risks to which they are exposed.
- The lone worker knows what to do if something goes wrong.
- Someone else knows the whereabouts of the lone worker and what he/she is doing

17.0 Incident Reporting

17.1 All security related incidents / near misses should be reported on Datix and to the LSMS, if urgent but not criminal. A local investigation should be initiated by managers.

All incidents of crime should be reported to the local Police Station. The LSMS should be notified as soon as possible by telephone / email and by the completion an incident report form on Datix.

Examples of reportable incidents include, but are not limited to:

- Physical assault or verbal abuse by a patient, visitor or another member of staff towards a member of staff;

- Physical assault or verbal abuse by a member of staff towards a patient or visitor;
- Theft of staff or CCG property;
- Leaving workplaces open at the end of the working day;
- Damage to premises that was the result of criminal activity (including arson)

If you are in any doubt as to what is reportable and what isn't, you should contact the LSMS.

17.2 Assisting the Police with Investigations

From time to time the police may contact the CCG for information relating to an on-going investigation. An individual who is contacted in such a manner should refer the Police to the LSMS or the Chief Finance Officer.

Staff should obtain guidance from Information Governance on when and the extent of confidential information may be disclosed.

17.3 Learning from Incidents

The CCG will ensure that learning from incidents is reviewed and changes made to the relevant policy and procedural to prevent reoccurrence. This will be incorporated in the work plan of the LSMS.

Appendix 1

Reporting of Crime / Security Incidents

All staff have a responsibility to report any crime / breach of security. This reporting falls into the following categories:

NHS Leeds West CCG Premises – Units B5 – B9, WIRA House, West Park Ring Road, Leeds, LS16 6EB.
Where a crime/security incident of a serious nature occurs and is happening there and then, dial 9-999 and report to police, and then the Security Management Director or their Deputy should be informed.

Where a security/criminal incident is discovered, the information should be passed to the Security Management Director or their Deputy and the Local Security Management Specialist as soon as practicable.

Completion of an Incident Reporting Form via Datix (as per Incident Policy) and a copy should be forwarded to the Local Security Management Specialist.

External Locations
Where a crime/security incident of a serious nature occurs and is happening there and then, you should call the police immediately by telephoning 999.

Where a security incident is discovered, the information should be passed to the Security Management Director or their Deputy and the Local Security Management Specialist as soon as practicable.

Completion of an Incident Report Form (as per Incident Policy) and a copy should be forwarded to the Local Security Management Specialist.

Out of Hours
Where a crime/security incident of a serious nature occurs and is happening there and then, you should call the police immediately by telephoning 999.

Following this the incident should be reported to the Security Management Director or their Deputy and the Local Security Management Specialist as soon as possible.

Suspicious (suspect) packages
A suspect package is a package believed to contain a potentially harmful device or substance.

Any suspect package or letter when received must immediately be placed in isolation and away from water, chemicals, heated surfaces, naked flames and gaseous substances. It is more likely to be an incendiary device than a bomb; i.e. it is designed to start a fire.

Do not shake it, squeeze, or open the letter or package.

Turn off all air conditioners, fans, photocopiers, printers, computers and heaters within the room where the letter/package is located. Close all windows and evacuate the room, lock all doors and leave the key in the lock. Place a clearly visible warning on the door.

Any suspicious packages should NOT be moved and its position should be reported to the Security Management Director or their Deputy or a member of the Senior Management Team. Undertake initial investigation (without touching or moving the package) identifying:

- The listed owner of the package
- Visible wires or electrical components showing from the package, especially where the wrapping has been damaged
- Any greasy marks on the envelope or package
- If an unknown powder or liquid substance is leaking from the package
- Distinctive smells from the package e.g. almonds/marzipan or machine oil
- If the package when delivered was heavy for its size or has an uneven distribution of weight or has excessive wrapping
- If the package was delivered by hand from an unknown source or posted from an unusual place

If in doubt, and dialing from an internal CCG landline dial 9-999 (if dialing from a mobile or other phone dial 999) and report to police and evacuate the building without sounding the fire alarm and closing doors and windows behind you.

Do not use mobile telephones near suspect packages.

If you feel you may have been contaminated, go to an isolated room and avoid other people if you can. It is vitally important that you segregate yourself and others who may have come into contact with the suspicious package. It is unlikely that you have been contaminated and you will get medical treatment if required. Signs that people may have been exposed to a chemical incident are streaming eyes, coughs and irritated skin. Do not rub your eyes; touch your face or other people. Thoroughly wash your hands in soap and water as soon as possible.

Where convenient, fire assembly points can be used for the purpose of evacuation, but only if they are located at a distance of at least 400 metres from the suspected bomb site. Safe assembly points are best situated behind a solid building at a distance away from the blast site. The safe assembly point for any suspicious package will be advised to staff at the time of the evacuation.

Bomb threats

A bomb threat is a threat to detonate an explosive or incendiary device to cause property damage or injuries, whether or not such a device actually exists.

Most bomb threats are made over the phone and the overwhelming majority are hoaxes, often the work of malicious jokers, although terrorists do make hoax calls with the intent of causing alarm and disruption. Any hoax is a crime and, no matter how ridiculous or unconvincing, must be reported to the police.

Calls may be of two kinds:

- **Hoax threats** designed to disrupt, test reactions or divert attention
- **Threats warning of a genuine device** – These may be attempts to avoid casualties or enable the terrorist to blame others if there are casualties. However genuine threats can provide inaccurate information about where and when a device might explode.

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.

Any member of staff receiving a telephone threat regarding a suspect package or explosive device should obtain as much detail as possible from the caller.

The police should be informed immediately - dial 999 and report to police and.

Principles

1. Stay calm and listen
2. Obtain as much information as possible – try to get the caller to be precise about the location and timing of the alleged bomb and whom they represent. If possible, keep the caller talking
3. Ensure that any recording facility is switched on
4. Write down the number showing on the phone displace or when the caller rings off, dial 1471 (if that facility operates) to see if you can get their number
5. Immediately report the incident to the relevant manager or security team to decide on the best course of action in line with the Emergency Preparedness, Resilience & Response Policy and notify the police. If you cannot get hold of anyone, and even if you think the call is a hoax, inform the police directly. Give your impressions of the caller and an exact account of what was said.
6. If you have not been able to record the call, make notes for police. Do not leave your post – unless ordered to evacuate – until the police arrive. If you evacuate the building do so without sounding the fire alarm and closing doors and windows behind you.

Appendix 2

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:

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
THREAT LANGUAGE:		Well-spoken □	Irrational □	Taped □	Foul □	Incoherent □
CALLER'S VOICE:		Calm □	Crying □	Clearing Throat □	Angry □	Nasal □
Slurred □	Excited □	Stutter □	Disguised □	Slow □	Lisp □	Accent* □
Rapid □	Deep □	Familiar** □	Laughter □	Hoarse □	Other (Please specify)	

* What Accent?

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

Street Noises □	House Noises □	Animal Noises □	Crockery □	Motor □

Clear □	Voice □	Static □	PA System □	Booth □	Music □

Factory Machinery □	Office Machinery □	Other (Please Specify)

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 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