Shropshire Community Health
NHS Trust

Policies, Procedures, Guidelines and Protocols

Document Details	
Title	**Security Management Policy**
Trust Ref No	1541-69805
Local Ref (optional)	
Main points the document covers	This policy sets out the arrangements for the security management of the Trust's property and assets, in particular the assessment of security risks and controls.
Who is the document aimed at?	Staff with responsibility for the management of the Trust's property and assets
Author	Terry Feltus, Local Security Management Specialist
Approval process	
Approved by (Committee/Director)	Sarah Lloyd, Director of Finance
Approval Date	01 October 2021
Initial Equality Impact Screening	Yes
Full Equality Impact Assessment	No
Lead Director	Sarah Lloyd, Director of Finance
Category	General
Sub Category	Risk Management
Review date	01 October 2023
Distribution	
Who the policy will be distributed to	Key Managers
Method	Datix alert and publication on the Intranet
Document Links	
Required by CQC	Outcome 10, safety and suitability of premises
Required by NHSLA	No
Other	Health and Safety at Work Act Management of Health at Work Regulations Violence Prevention and Reduction Standards 2021

Amendments History		
No	Date	Amendment
1	July 2015	To remove reference to the obsolete Secretary of State Directions
2	July 2015	To reflect on, and include reference to, The Standards for Providers Guidance issued by NHS Protect
3	July 2015	Adjusted structure chart to reflect current reporting arrangements
4	July 2015	Updated "Bomb Threat" procedures
5	July 2015	To update policy with new Trust Director details and title

Amendments History		
No	Date	Amendment
6	January 2018	Document amended following Department of Health's decision to remove NHS Protect responsibility for overseeing and supporting security management work
7	January 2018	To add a section on Terrorism Incidents
8	January 2018	To add a section on Security of Motor Vehicles and Bikes
9	January 2018	To add a section on Site Access and Parking
10	March 2019	To update policy with Lead Director's new title (Director of Finance and Strategy)
11	March 2019	To include reference to the role of the Trust Associate Director of Finance in overseeing security management related work
12	March 2019	To amend all references relating to data protection to the Data Protection Act 2018
13	March 2019	To include the Local Security Management Specialist contact details
14	March 2019	To remove references to NHS Protect
15	March 2019	To add 'CCTV image release' section
16	March 2019	To add 'parking charge notice' section
17	September 2021	Removal of remaining references to NHS Protect
18	September 2021	To add reference to General Condition 5.9 of the NHS Standard Contract to have regard to the NHS Violence Prevention and Reduction Standard
19	September 2021	To change 'Corporate Risk Manager' to 'Head of Governance and Risk'
20	September 2021	To add requirement for 'all area access' card/fob to be held on crash trolleys.
21	September 2021	To add reference to Schedule 2 part 1 5 (3)(a or c) of the Data Protection Act request for CCTV footage release.
22	September 2021	To update policy with Lead Director's new title (Director of Finance)

Security

Management Policy

Index

1 Introduction

1.1 Security affects everyone who uses, or works within, the NHS. The security and safety of staff, professionals, patients and property must be a priority within the delivery and development of health services. All of those working within the NHS have a responsibility to be aware of these issues and to assist in preventing security related incidents and losses.

1.2 Reductions over time in losses or incidents, through the consequences of violence, theft or damage will lead to more resources being freed up for the delivery of better patient care and contribute to creating and maintaining an environment where staff, professionals and patients feel and are more secure.

1.3 In line with published guidance, Shropshire Community Health NHS Trust is committed to providing the best possible protection for its patients, staff, visitors and property.

1.4 The Trust is required under General Condition 5.9 of the NHS Standard Contract to have regard to the NHS Violence Prevention and Reduction Standard.

2 Purpose

2.1 The purpose of this Policy is to outline the Trust's approach to security in order to provide a safe and secure environment for those who work in, or use, NHS services, as defined in the introduction.

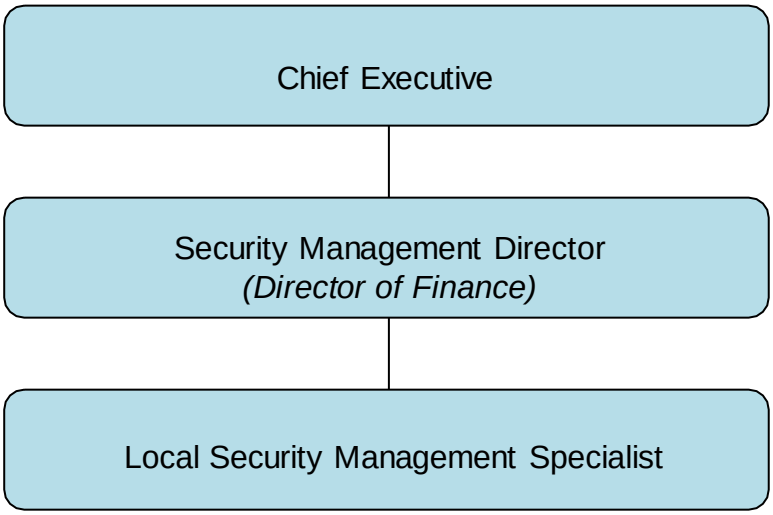
3 Definitions

LSMS	Local Security Management Specialist, appointed by the Trust and accredited by the nominated Professional Accreditation Board.
SMD	Security Management Director.

4 Duties

4.1 Roles and responsibilities of key individuals directly involved in the security management process is shown below. Work undertaken by the identified individuals is pivotal in ensuring that related compliance and directions are met. The Chief Executive has overall responsibility and accountability, on behalf of the Board, for security, and must ensure that the organisational commitment to security management is fully met and monitored.

Figure 1: Security Management Structure



- **Executive Director: (Director of Finance)** shall undertake the role of Security Management Director and shall take overall responsibility for overseeing security management work and ensuring that any relevant security management guidance is complied with. The Director of Finance will oversee the work of the nominated Local Security Management Specialist for the Trust on a daily basis on all security related matters.

- **Local Security Management Specialist:** their principal role is to deliver security management work locally, to comply with published guidance, and will be responsible for:-

  - Providing advice, support and assistance regarding security management issues and ensuring all work is undertaken in line with any relevant reporting requirements.
  - Actively promoting security management issues, working closely with all staff to ensure a pro-security culture is developed and maintained.
  - The collection and analysis of all information relating to security incidents in order to identify trends and implement incident reduction strategies.
  - The review and investigation of all breaches of security and related incidents as appropriate.
  - Ensuring that security management work is integrated into Trust risk management procedures.
  - The inspection and security/audit review of Trust premises and related work practices.
  - Liaison with Police Services, Crown Prosecution Service (CPS), Counter Terrorism Officers and any other relevant external agencies.

- **Violence Prevention and Reduction Lead:** responsible for compliance with the Violence Prevention and Reduction Standards

- **Trust Managers, Heads of Department and Team Leaders**: responsible for leading on, and promoting, security within their area(s) of responsibility. In particular they will be responsible for:-

  - Nominating a "local responsible person" for each of the premises under their control.
  - Producing and implementing local security procedures and protocols, in line with the Trust's Security Management Policy. (The "Security Protocol" template can be found at Appendix 1.)
  - Undertaking security risk audits annually, in accordance with the Trust's Risk Management Policy and acting to remove or reduce (as far as is reasonably practicable) any security risks identified, in consultation with the Trust's LSMS where appropriate. (Further guidance can be found in the Risk Management policy.)
  - Ensuring all security measures implemented as a result of the risk assessment are reviewed when circumstances change, and an annual review of security measures and procedures detailed in the risk assessment is carried out.
  - Ensuring all breaches of security and criminal acts are reported in accordance with the Trust's Incident Reporting Code of Practice. The LSMS's advice should be sought where it is necessary to report incidents to the Police.

- **Trust employees and Contractors:** must:-

  - Conform to the Trust's Security Management Policy and any local protocols put in place to safeguard the security of property, and the personal safety of themselves and others.
  - Ensure that all security-related incidents are reported in accordance with the Trust's Incident Reporting Policy.

- **Nomination of Buildings Security Lead (Local Responsible Person)**

  Service managers must nominate a lead (Local Responsible Person) for security for each of the buildings under their control. This person will be responsible for the day to day security management of the premises according to the arrangements identified by the risk assessment detailed below. Where there is multi-occupation by services the relevant service manager must agree an overall lead. It is likely that the Local Responsible Person will take the lead for fire and health and safety within the premises as well as security. The Local Responsible Person must draw up a security protocol. A pro-forma for this is detailed in Appendix 1.

5 Risk Assessments

5.1 A security risk assessment will be carried out for all premises that the Trust manages by the appropriate manager/head of department/team leader identified by the Service Manager, using the Security Risk Assessment pro-forma which can be found at Appendix 2 of the Security Management Policy.

5.2 The purpose of the risk assessment is to identify any shortfalls in the security arrangements that will increase the risks to the Trusts property and assets. Where shortfalls are identified, and it is reasonably practicable to do so, further arrangements will need to be identified.

5.3 Significant findings should be entered onto the departmental risk assessment held on the Datix risk register. The pro forma must be attached to the risk assessment as a document.

6 Action Plans

6.1 If the assessment has identified further arrangements to be put into place an action plan will need to be developed, in consultation with the LSMS where necessary. Actions should be recorded on the action plan attached to the Datix record. The minimum content of the actions should be:

- What needs to be carried out.
- Who will carry this out.
- When it will be carried out by.

7 Review of Action Plans/Recommendations

7.1 Completed risk assessment pro-formas should be forwarded to the LSMS along with any action plans formulated as a result of the assessment. The Service Manager, in conjunction with the Local Responsible Person, will monitor progress against identified actions and ensure that these are recorded on the Datix action plan.

7.2 The Head of Governance and Risk will produce a monthly report detailing actions which are due or overdue. This will be forwarded to relevant service managers who will ensure that the plan is updated.

7.3 The LSMS will follow up any significant actions required when they deem it necessary to do so.

8 Incident Reporting

8.1 All security incidents must be reported according to the Incident Reporting policy using the online reporting form.

8.2 Managers review all incidents and action as appropriate. Significant incidents will be reported to the LSMS immediately. All other security incidents will be reported to the LSMS when reviewed by the Head of Governance and Risk/Assistant.

8.3 The police should be involved where criminal activity has taken place, consulting the LSMS as necessary.

9 Violence and Aggression/Physical and Non-Physical Assault

9.1 It should be recognised that the management of violence and aggression will always present a significant risk to the Trust due to the nature of the client/patient base to whom care is delivered. The Trust recognises and is committed to implementing relevant control measures to mitigate against identified risks related to violence and aggression.

9.2 The arrangements for the management of violence and aggression are detailed in the Violence and Aggression, including Lone Working Policy.

Police investigation into violent incidents

9.3 The Trust will actively encourage and support the Police to investigate reported incidents of violence and aggression perpetrated by patients, in such cases where it has been identified that the perpetrator was likely to have known what they were doing was wrong and the assault was not due to their "clinical condition". It should however be recognised that in order for the police to initiate such an investigation they will require the following information: -

- Did the perpetrator have capacity to understand their actions?
- Is the perpetrator fit to be interviewed?
- Is the perpetrator fit to plead?

9.4 Such information should be sought from the Responsible Clinician and the LSMS should facilitate the gathering of such information, but where the appropriate clinician is unable to provide this information the LSMS shall refer the case to the Trust's Caldicott Guardian, for further guidance and direction.

9.5 Where the police decline to investigate an incident under these circumstances the LSMS may refer the case to the Trust SMD for further guidance and direction.

9.6 All Police investigations shall be undertaken in line with statutory directions issued through the Police and Criminal Evidence Act (PACE) 1984. The LSMS shall be the nominated Trust contact with the Police during such investigation and shall also provide, where appropriate, support and professional guidance to all staff or persons involved with such investigation.

9.7 Additional Guidance is given in Appendix 3:

10 Consultation

10.1 This policy has been developed in conjunction with the LSMS and Estates Officer. Consultation has been carried out with Service Managers.

11 Monitoring Compliance

Element to be monitored	Lead	Tool	Frequency	Reporting arrangements	Acting on recommendations and Lead(s)	Change in practice and lessons to be shared
Duties	LSMS	Annual Report	Annually	The LSMS will prepare an annual report on the effectiveness of the security management arrangements which will be reviewed by the Audit Committee, and the Quality and Safety Group	The LSMS will report overall issues to be actioned, to the Audit Committee/Quality and Safety Group and individual issues to Service Managers. Actions will be allocated according to their nature	Lessons will be shared by the Quality and Safety Group to service leads/managers
How the organisation risk assesses the physical security of premises and assets	Head of Governance and Risk	Audit	Annually	The Head of Governance and Risk will organise an audit of required risk assessment. A summary report will be prepared for the Quality and Safety Group	Head of Governance and Risk will make recommendations where improvements are needed to service managers and leads	Lessons will be shared by the Quality and Safety Group to service leads/managers
How action plans are developed as a result of risk assessments	Head of Governance and Risk	Risk moderation	Ongoing	Head of Governance and Risk will review all risks entered on the risk register to ensure appropriate actions have been developed. Feedback will be given to lead for risk area	Risk leads, in conjunction with service leads//managers will formulate actions where needed	Lessons will be shared by the Quality and Safety Group to service leads/managers
How actions plans are followed up	Head of Governance and Risk	Report	Monthly	Any problems with implemented actions raised with CSMs/ Service Managers	CSMs/ Service Managers will make recommendations as necessary and ensure that line managers complete identified actions	For significant issues raised through Senior Management Group and through team meetings in individual areas.

12 References

12.1 Violence Prevention and Reduction Standards

13 Associated Documents

13.1 This Policy, and all direction and guidance included in it, should be read in conjunction with relevant Trust Policies and Procedures which include:-

- Security Management Strategy.
- Health and Safety Policy.
- Violence and Aggression, including Lone Working, Policy.
- Risk Management Policy.
- Whistleblowing Policy.
- Incident Reporting Policy.
- Emergency Response Arrangements Policy.
- Anti-Crime Specialists and Human Resources Advisory Team Protocol.
- Anti-Crime Specialists, and Internal Audit Protocol.

Appendix 1: Security Protocol

Please complete the information below for each location where Trust services are provided. This information should be made available to all staff operating from this location.

Address	

Responsibilities			
Manager (NB: This should be the service manager. This person may be based elsewhere)			
Name		**Contact No**	
Deputy *(NB: This should be a manager, team leader, etc who is based on-site at this location)*			
Name		**Contact No**	

The above manager shall be responsible for:-

- producing robust protocols in respect of security of the above premises, which should cover building security (site specific), personal and property security; see "Policies and Protocols" section below
- security incident reporting

The above deputy shall be responsible for ensuring:-

- all staff are aware of, and comply with, the protocols which relate to their work environment
- every security-related incident is appropriately reported in accordance with Trust guidelines
- risk assessments are carried out as appropriate

Staff Responsibilities

Security is the responsibility of <u>all</u> staff, irrespective of their role within the Trust. All staff should:-

- understand their roles and responsibilities in respect of security of both the premises and their personal safety and property whilst at their place of work – see "Policies and Protocols" below
- report all security-related incidents, no matter how minor:-
    - to their manager
    - through the Trust's Incident Reporting system (Datix)
    - to the Trust's LSMS and/or the Police as appropriate

Policies and Protocols
Building and Premises security (site specific) • Locking and unlocking premises, and alarming (where appropriate) • Key holding responsibilities and the management of access control systems (eg fobs) • Visitors to premises • Security of Trust property • Monitoring and maintenance of CCTV systems (if applicable) *(NB: the above procedures should be expanded to provide guidance to be adopted under each heading.)*

Personal Safety and Security of Property
• Lone working
• Violence and Aggression
• Security of Property
  ○ Trust (eg laptop, mobile phone)
  ○ Patient
  ○ Personal (eg wallet, car keys)
(NB: the above procedures should be expanded to provide guidance to be adopted under each heading.)

NB: Procedures and protocols should be produced in accordance with the Trust's Security Management Policy, and in consultation with the Trust's LSMS where necessary.

Appendix 2: Security Risk Assessment

Premises Address	
Assessor	
Date	
Review Date	

POLICIES	Yes	No	N/A	Remarks/Comments/Actions
Security Management Policy				
Security Management Strategy				
Violence & Aggression, including Lone Working, Policy				
Are staff aware of the above policies?				
Are staff briefed on the above policies, and how often?				
Are staff aware of the requirement to wear staff ID badges at all times whilst on NHS business?				
PERIMETER	Yes	No	N/A	Remarks/Comments/Actions
Does the site have a perimeter fence with gates/barrier?				
What type of fencing, and what state of repair is it in?				
Does the fencing prevent unauthorised access?				
Are the gates/barrier used to control access to the site during normal working hours?				
Are the gates secured at night?				
Is the site secure out-of-hours?				

Is there signage around the site warning against illegal access to the site?				
EXTERNAL SECURITY - LIGHTING	Yes	No	N/A	Remarks/Comments/Actions
Is there security lighting installed around the site?				
Does the security lighting support CCTV?				
Is the level of security/ street lighting adequate for the site?				
Are there any unlit areas which cause concern?				
Are any of the security lights obstructed or damaged?				
Are movement sensors/ PIR security lights fitted? If yes, for what purpose and where?				
EXTERNAL SECURITY - GENERAL	Yes	No	N/A	Remarks/Comments/Actions
Is there any evidence of unauthorised use of the site, eg antisocial behaviour, graffiti, alcohol/drug abuse?				
Is there a grounds maintenance programme in place for gardens, shrubs, trees, hedges?				
Do staff have access to on-site parking?				
Is the car park maintained, secure and patrolled if on site?				

BUILDING - SECURITY	Yes	No	N/A	Remarks/Comments/Actions
Is the building fitted with external security lighting?				
Does the building have any areas which are not covered by security lights/CCTV that may be used for antisocial behaviour?				
Is the building fitted with an intruder alarm?				
If yes, is the alarm monitored by an approved alarm monitoring centre?				
Does the alarm company provide a key holder response to all alarm activations?				
Is there a nominated person responsible for security and key holding, with a deputy in the event of an alarm activation?				
Does the building have signage directing visitors to the main reception and/or public access points?				
Are all external doors fitted correctly, and do they open and shut as required, ie are they fit for purpose?				
Are all doors fitted with appropriate locks which meet the minimum requirements of being at least a 5-lever mortise or similar hook lock, fitted top and bottom?				

If the building is fitted with either a digital or electronic key pad as its main means of access, is there a back-up system in place in case of failure?				
In the case of key pads, are the codes changed on a regular basis? If yes, how often?				
Are doors which are not used as primary access and egress kept locked and alarmed?				
Are all windows securable and do they meet minimum security standards?				
Where appropriate, are window opening restrictors/limiters fitted to prevent access?				
Does the building have any flat roofs?				
Can the flat roof be accessed from the ground?				
Does the building have fire escapes to upper floors?				
Are there measures in place to restrict access to fire escapes from ground level?				
CCTV - SECURITY				
Does the system provide external coverage?				
Does the system provide internal coverage?				
Are images recorded?				
Is CCTV monitored?				

Are the perimeter/ access points covered by CCTV?				
Does the CCTV face any residential property?				
Is CCTV signage displayed around the site?				
Is there a maintenance contract in place for the system?				
Is the system registered with the Information Commissioner's Office, and does it comply with the Data Protection Act?				
ACCESS - SECURITY				
Is visitor access to the building/premises managed?				
Does the building have a staffed reception?				
Is the receptionist a lone worker?				
If yes, does the receptionist have access to a panic button or personal attack alarm?				
Is access to the building via an intercom?				
Does the intercom have a camera?				
Are visitors escorted to and from reception or access point?				
Are visitors required to book in, and are they issued with a security badge?				
Is reception/access point covered by CCTV?				

PERSONAL SAFETY - SECURITY	Yes	No	N/A	Remarks/Comments/Actions
Have staff attended Conflict Resolution training?				
Have frontline, (i.e. patient facing), staff attended Management of Actual or Potential Aggression (MAPA) training?				
Have staff received security/personal safety training?				
Where appropriate, do staff have access to personal alarms?				
Are staff aware of the Incident Reporting policy?				
Are staff aware of the Violence & Aggression, including Lone Working, Policy?				

Additional Comments:

Appendix 3: Additional Guidance

a) New Builds, Redevelopments or changes of use of existing premises

To support this and ensure that effective measures to enhance physical security are implemented from the outset, the LSMS should be consulted with and informed at the earliest opportunity of any planned new builds, redevelopments or change of use so that appropriate advice and guidance can be sought. The LSMS should then be involved at all stages of the planned redevelopments up to the point of when the redevelopment is signed off and functional.

b) Responsibilities of Trust Managers, Heads of Department, Team Leaders:

To ensure that effective procedures and control measures are implemented for their area(s) of responsibility that enhances the physical security of the premises/building. Such measures will include the following:-

- Undertaking risk assessments for all areas where it has been identified that the physical security of a building could be compromised (ie access control points or windows). Specialist advice, on request, for this process shall be afforded by the LSMS.
- Implementing and monitoring effective working practices that support the risk assessment process and ensuring that all improvements and control measures required are implemented, ensuring that security is not unduly compromised.
- Where it is identified that a redevelopment or change of use is planned then the LSMS is to be consulted and involved from the outset to ensure that security is not unduly compromised and that appropriate control measures are implemented.

c) Responsibilities of Staff:

To play an active role in the physical security of their workplace. This will include adherence to all local procedures by ensuring that their workplace is maintained as a safe and secure environment, and that any concerns they have are reported to their line manager.

d) Responsibilities of the Local Security Management Specialist (LSMS):

To advise and review all measures to be implemented relating to the physical security of Trust premises and assets. This will include:-

- All new builds
- Redevelopments
- Changes of use
- Existing premises

In order for this to be achieved, the LSMS should be involved at all stages of the planning process where it has an impact on security

The LSMS will provide a report following any security review which will outline any findings, actions and recommendations to all relevant persons.

e) Staff and Visitor Identification

Staff Identification

- Whilst on Trust business, all staff will have available on their person, at all times, a valid Trust ID Card.
- ID Cards will bear the Trust name, the individual's name & designation and photographic likeness of the individual.
- Lost or damaged cards must be reported to the individual's line manager immediately and a replacement sought without delay.
- ID Cards must be surrendered to the individual's line manager on leaving the employment of the Trust.
- Individual managers who employ or allow temporary workers, volunteers or contractors on their premises shall ensure that these persons are bona-fide and if these persons are working within the area for a considerable period of time then consideration should be given to issuing them with a Trust ID Card.

Visitor Identification

- Individual Wards/Departments/Units shall operate a Visitor recording system that requires all visitors to Trust premises to sign in and out of such premises.
- Visitor recording systems may vary between sites and areas but all should record similar information that will include the visitor's name, the date and time, the purpose of their visit and the registration of any vehicle parked on the premises.
- All visitor recording systems will include reference to essential safety information that must be brought to the attention of the visitor on their arrival, ie action to be taken in event of fire or other emergency.

f) Access Control Systems/Key Security

Access Control Systems

Where access control systems are utilised on Trust premises it shall be the responsibility of the designated Manager of the Ward, Unit or Department to ensure that local protocols are in place to ensure correct procedures and working practices are adopted for the use and management of such systems. The following information shall detail guidance, direction and best practice to be adopted by staff where access control systems are utilised.

- Doors that are designated access control points (i.e air lock door entry into restricted area) should be kept closed at all times and should never, for any reason, be propped open.

- Keys or access control proximity/swipe cards that have been allocated to an individual member of staff should never be lent to, or used by another person.
- Staff should always be aware of, and safeguard against potential unauthorised access into restricted areas and not allow unauthorised persons attempting to tailgate through access control points into such areas.
- Premises and individual departments vacated for any length of time must be secured to restrict any form of unauthorised entry.
- Combinations for keypad control locks should never be given to unauthorised persons and should be changed at least twice a year.
- All access control points should be checked on a regular basis to ensure that they are working correctly and are properly secure.
- Where swipe card/fob access systems are in use in patient environments, an 'all area access' card/fob must be kept on the medical emergency response trolley. The card/fob must only be used in the event of an emergency and shall form part of the daily trolley check regime.

Control of Keys/Access Fobs

Where keys/fobs are utilised by staff to control access into restricted areas the following guidance shall be applied:-

- The issuing, recovery, recording and security of departmental keys/fobs is the responsibility of Ward/Unit/Departmental Managers.
- Staff should be aware of all procedures relating to their area of work for the issue, security and use of keys/fobs.
- Duplicate keys must be available in a designated secure place for use in the event of an emergency.
- Keys should not be able to be identified easily and should not be tagged with the name of Ward/Department/Site to which they belong. For example, colour coding is a secure method of identification providing the explanatory chart is stored separately from the keys themselves.
- Managers should keep a list of keys/fobs issued to staff and should ensure that they are returned prior to staff leaving.
- Managers need to consider whether to replace locks if keys are not returned.
- Managers should ensure that fobs are deactivated when a member of staff leaves the Trust.
- Where keys/fobs are issued to contractors for access, a record should be kept. This should include details of: the company, the individual, the date and time of issue and return.

g) Security Alarm Systems

Building

When correctly installed and monitored, security alarm systems can help prevent losses of property through criminal activity. It should however be recognised that an alarm system can only act as a deterrent to crime.

To offer protection, an effective response to alarm activation is essential. There are three levels of response:-

- Standalone Alarm

  Building is alarmed **but not monitored** by any alarm monitoring centre. No response by Security Company or police. Response is dependent upon any report to the police by a member of the public, and what information is provided by them.

- Monitored by an alarm monitoring centre, with key holder response

  Centre will call out a nominated on-call manager to investigate the reason for the alarm activation. (A 20 minute response time is recommended).

- Monitored by an alarm monitoring centre, with security company response

  Centre will contact the nominated security company who will act as first response (will have keys/fobs). The call out of the on-call manager and/or the police is dependent upon whether the alarm activation is as a result of criminal activity. If no criminal activity is found, the security company will reset the alarm and inform the premises manager the next working day.

  Advice on the appropriate type of alarm system and monitoring should be sought from the LSMS.

  The designated Manager of the Ward, Unit or Department is to ensure that all staff are aware of the correct procedures for arming and disarming the alarm. This procedure should be incorporated into the Security Protocol for that premises.

Lone Worker Devices

The Trust are currently assessing the potential introduction of lone worker devices. For more information, please contact your Line Manager or LSMS.

h) CCTV

CCTV Guidance

CCTV systems are in use at a number of Trust premises. These systems have been installed following security risk assessments which have identified the need for CCTV in order to protect premises, staff, patients and visitors where appropriate.

It should be noted that CCTV systems are only a deterrent to reducing crime and are subject to limitations as posed by: environment, siting, quality of the system, and the level of monitoring and recording.

CCTV is not used to routinely monitor staff, but images will be captured and recorded at sites where CCTV is active.

CCTV images may be used in police investigations or internal disciplinary proceedings following a serious incident.

Where systems are installed, they shall be managed by the designated manager for that area.

The procedure for operating and monitoring of the CCTV system will be incorporated into the Security Management Protocol for those premises.

Where security incidents have occurred, the designated manager or LSMS should review the CCTV footage to establish whether evidence relating to the incident has been recorded. This footage should be saved and provided as evidence in any subsequent investigation.

The designated manager responsible for monitoring the CCTV should ensure that the system is not abused or misused.

Legal Guidance

The Security Management Director (SMD) and/or the Director responsible for Data Protection shall be the appointed person by the Trust as the appropriate Director who has overall legal responsibility for CCTV systems operated by the Trust.

The SMD will ensure that the LSMS has oversight of procedures supporting the operational use of CCTV systems utilised by the Trust to ensure compliance with legislation and guidance and provide the SMD assurance that relevant requirements are being met.

The SMD and LSMS will ensure that the following legislative guidance on the use of CCTV systems by the Trust is implemented:-

- That all CCTV systems operated by the Trust shall be carried out in accordance with legislative guidance and codes of practice in relation to the following:-
    - The Data Protection Act 2018
    - The Human Rights Act 1998
    - The Regulation of Investigatory Powers Acts 2000
    - The Information Commissioner's Office (ICO) CCTV Code of Practice
- That all staff involved in the operation or monitoring of CCTV systems operated by the Trust have a responsibility to comply with associated legislation and guidance.

Release of Images

CCTV images will only be released following an appropriate subject access request in line with the Trust's Information Governance Policy.

Images requested for the prevention and detection of crime will only be released following the receipt of a Schedule 2 part 1 2 (1)(a) of the Data Protection Act 2018 request (Previously Section 29(3) The Data Protection Act 1998).

Images requested for use in connection with (potential) legal proceedings or establishing, exercising or defending legal rights will only be released following the receipt of a Schedule 2 part 1 5 (3)(a or c) of the Data Protection Act request.

i) Lockdown Procedures

In line with responsibility to ensure a safe and secure environment, guidance has been developed to explain the planning and execution of a lockdown in NHS healthcare sites.

The Trust will develop plans and procedures based on such guidance to achieve hospital lockdown. Detailed information can be found in the Trust's "Emergency Response Arrangements" Policy.

Recognition is also given to the law of the land in respect of Civil Contingencies Act 2004, Public Health Act and articles 5 and 12 of the Human Rights Act.

Defining site/building lockdown

For the purpose of this policy, a lockdown is defined as:-

The process of controlling the movement and access – both entry and exit – of people (staff, patients and visitors) around the Trust or other specific Trust building/area in response to an identified risk, threat or hazard that might impact upon the health and safety/security of patients, staff and assets or, indeed, the capacity of that facility to continue to operate. A lockdown is achieved through a combination of physical security measures and the deployment of personnel.

j) Security of Property (Trust Assets, Patient, Personal)

Trust Property

- It is the responsibility of all managers to ensure a comprehensive inventory of all Trust equipment is maintained for their area of responsibility and kept up-to-date as appropriate. Equipment moved between premises and departments should be recorded in and out as appropriate.
- Equipment capitalised under the Trust's accounting policies should always be included in the Trust's Asset Register operated by the Director of Finance. All Managers have a responsibility to co-operate with the Director of Finance to ensure that the Asset Register is complete, accurate and timely.
- High-risk and business critical assets under £5000 need to be captured on departmental asset registers.

- Staff should ensure adequate measures are taken to protect Trust equipment and that all items of equipment are not left vulnerable to potential theft, loss, malicious/criminal damage or misuse.
- When Trust equipment is not in use all items should be stored in a secure environment and not left on general view. When Trust equipment is carried in vehicles it should always be safeguarded by placing items out of sight and locking the vehicle when unattended.
- It is the responsibility of all managers to ensure robust control systems are in place for consumables (eg stationery, medical supplies, disposable sanitary products, etc), in order that all items are properly accounted for.
- All incidents of theft, loss, malicious/criminal damage and misuse of Trust equipment should be reported to the LSMS for further investigation/action.

Patient Property (Wards & Residential Settings)

Property belonging to patients and clients can be subject to theft, malicious damage or misuse. All patients and clients should be encouraged to leave property or personal items of a valuable nature at home or hand them in for safekeeping. Detailed instructions on procedures for safeguarding patient property against theft, malicious damage or misuse is included in the Trust's Standing Financial Instructions and Finance Procedure I17: Patients Property – Cash & Valuables. All staff must also ensure that the following points are adhered to:-

- Record all property that is formally handed over and ensure the patient is issued with a receipt, ensuring as much detail as possible is recorded.
- To advise patients and their relatives/carers of the risks if they do not formally hand property over for safekeeping.
- A patient's property form must always be completed even if patients do not hand over property.
- If patients are likely to be away from the Ward/Unit for a period of time, staff must encourage them to hand over all valuables for safekeeping.

Staff Property

All staff are responsible for their personal property and are advised to make use of locked facilities where available.

It is recommended that only essential items and minimum quantities of cash should be brought to work.

Staff should not leave valuable items unattended at any time.

Staff should be aware that the Trust does not take responsibility for losses or damage to personal property at work.

k) Firearms and Weapons

Whilst it is rare, incidents involving firearms or offensive weapons may occur in both the community or on Trust premises, therefore staff should be aware of the

risks of becoming involved in such an incident. It should be recognised that each incident has the potential to cause alarm, distress or fear and be extremely serious. Such incidents are more likely to occur in the community due to staff being lone workers.

Where staff are lone workers, it is the responsibility of all managers (in consultation with the LSMS) to ensure that robust lone working procedures are in place and that appropriate risk assessments have been completed to ensure risks have been eliminated or minimised.

The following guidance is to be adopted on Trust premises in the event of an incident of this nature, and should be included in the Security Protocol developed for each premises, and should be followed by Trust staff should they find themselves under threat from firearms or weapons:-

Personal Safety

Your safety and the safety of others in the vicinity are a matter of priority and, where possible:-

- Remove yourself and others from the immediate threat area, staying as calm as possible – see “Before Police Arrival at the Scene” below.
- Call the police without putting yourself at risk – see “Contacting the Police” below.
- If you are unable to contact the police yourself, as discreetly as possible, attempt to raise the alarm to others in the vicinity.

Contacting the Police

All incidents involving firearms or weapons are a matter for the Police and should be reported to them immediately by dialling 999.

The person (member of staff) who calls the Police should give as much relevant information about the situation as possible including:-

- The nature of the firearm or weapon (eg rifle, knife, gas spray etc).
- Who has (if name known) possession of the firearm or weapon.
- Description (if name not known) of the person who has possession of the firearm/weapon.
- Exact location of the incident and where the offender physically is within that location.
- Whether any shots have been fired or weapons used.
- Any injured persons or potential imminent risk to personal safety or life.

Before Police Arrival at the Scene

Whilst it is accepted that this may be extremely difficult or potentially dangerous, the following information will give staff guidance on how to deal with the situation:-

- Make an immediate escape if safe to do so, but do not attempt if it would compromise your safety.
- Stay as calm and composed as you can, engaging with the individual if appropriate.
- Do not say or do anything that is likely to escalate or enflame the situation.
- Do not use force or attempt to disarm a person unless life or personal safety is in immediate danger.
- If the incident is on Trust premises the Lockdown Procedure should be implemented.
- A phased evacuation of the immediate and subsequent areas should be implemented where safe to do so, in line with the Trust's Lockdown Procedure.

Following Police Arrival at Scene

On arrival, the police will assume full command and control of the incident **WITHOUT EXCEPTION**.

The following Trust staff should be on hand to assist the police as appropriate:-

- Premises Manager/Estates Manager.
- Relevant Manager or on-call Manager out of hours.
- LSMS.
- Trust Health Emergency Management Specialist.
- Trust Communications Manager.
- Witness(es) to the incident.

l) Bomb Threat or Similar Risks or Threats

Bombs or improvised explosive devices (IED) are used by those wishing to cause fear, economic loss, disruption or personal injury, and can be either identified by the receipt of a telephone call/message and/or a suspect package being found.

Bombs and IEDs can take many forms, eg letter bomb, packages, bags, etc. The following guidance gives direction where it has been reported that a bomb or suspect package has been found on Trust premises.

Similarly, a hoax bomb threat can cause a great deal of disruption to the Trust's ability to deliver effective care. Where a bomb or similar hoax occurs, the matter must always be reported to the Police, if they are not already involved. The LSMS should act as the liaison point with the Police to support any subsequent investigation they undertake into a hoax bomb threat.

Actions to be taken in the event of a Bomb Threat

All bomb threats are a matter for the Police who must be called using the 999 emergency services as soon as possible. A checklist of actions to be taken in this situation can be found in this Appendix.

Search and Evacuation

Guidance on search and evacuation procedures can be found in this Appendix, as can instructions on how to identify and deal with a suspicious package.

An Incident Algorithm can be found on page 35 of this document which demonstrates the process to be followed in the event of any incident.

The decision to evacuate a building/part-building lies with the senior manager on site, in consultation with the Security Management Director/On-Call Director and/or the Health Emergency Management Specialist and/or the LSMS.

Incident Room

Each property should identify a room or area which can be used as an Incident Room in the event of an emergency situation. An alternative area should also be identified as back-up if the primary location is within the affected area.

Decision to Stand Down/Reoccupy

A decision for the incident to be stood down should only be made by the Police. Once such a decision has been communicated then consideration should be given for the premises to be reoccupied in a safe and orderly manner.

m) Staff Bomb Alert Procedure

If someone rings your telephone with a bomb threat:-

DON'T PANIC - obtain as much information as possible **DON'T HANG UP** - even when the caller does.

DO tell your Line Manager.
DO inform the switchboard - using a separate telephone.
DO go to the Incident Room as detailed below:-

Incident Room

First Choice	
Second Choice	

If you Find a Suspicious Package or Device:-

- DO NOT touch or move it.
- Remove or turn off all hand-held communications devices in the vicinity.
- If the device is concealed, leave a distinctive marker nearby.
- Raise the alarm.

Actions to be Taken on Receipt of a Bomb Threat

1.	Switch on voice recorder (if connected). Record the exact wording of the threat.		
2.	Ask these questions:-		
	i	Where is the bomb?	
	Ii	When is it going to explode?	
	iii	What does it look like?	
	iv	What kind of bomb is it?	
	v	What will cause it to explode?	
	vi	Did you place the bomb?	YES/NO *(delete as appropriate)*
	vii	If Yes, why?	
	viii	What is your name?	
	ix	What is your address?	
	x	What is your telephone number?	
3.	Record time call completed		
4.	Record your name, job title and telephone number of person informed		
5.	Inform the Security Management Director /the On-Call Director, the LSMS, and Health Emergency Management Specialist Time informed		
6.	Contact the Police by Dialling 999: Time informed		

NB: This part should be completed once the caller has hung up and the Security Management Director/On-Call Director/Health Emergency Management Specialist/LSMS and the Police have been informed.

7.	Date and Time of Call				
8.	Length of Call				
9.	Number at which call was received (including extension number)				
10.	**About the caller** (if it is possible to state)				
	i	Sex of caller?	MALE/FEMALE *(delete as appropriate)*		
	ii	Nationality?			
	iii	Age?			
	iv	Threat language *(tick all applicable)*			
		Well-spoken?		Irrational?	
		Abusive?		Unintelligible?	
		Message read from a text?	YES/NO *(delete as appropriate)*		
		Taped message?	YES/NO *(delete as appropriate)*		
	v	Caller's voice *(tick all appropriate)*			
		Calm?		Crying?	
		Clearing throat?		Angry?	
		Nasal?		Slurred?	
		Excited?		Stutter?	
		Disguised?		Slow?	
		Lisp?		Rapid?	
		Rapid?		Deep?	
		Hoarse?		Laughter?	
		Accent?		*(What accent?)*	
		Familiar?		*(Who did it sound like?)*	
	vi	Background sounds *(tick all appropriate)*			
		Street noises?		House noises?	
		Animal noises?		Crockery?	
		Motor?		Clear?	
		Voices?		Static?	
		Music?		PA System?	
		Telephone booth?		Factory machinery?	
		Office machinery?		Other *(please specify)*	
11.	Comments				

Signature		Date	

Initiating a Search and Evacuation Procedure

Search Priorities

All heads of department will be informed whether the threat is specific or non-specific. Department managers will instigate a full search of all areas under their control. On completion they will report to the designated Incident Room.

What are they to look for?

Any unidentified object that:-

- should not be there;
- cannot be accounted for;
- is out of place

How to Search

The search should be carried out in a logical and thorough manner so that no part of their department and immediate vicinity is left unchecked. Anything untoward should be challenged but not disturbed.

Room Search

A search should begin at the entrance to the area. Each searcher or team should first stand still and look around the room. They should note the contents of the room and make a quick assessment of those areas which will need special attention. They should look for any unusual lights (including small light sources known as LEDs which are often used in terrorist bombs). They should also listen carefully for any unusual noises, particularly ticking or whirring sounds. If anything unusual is seen or heard, the searcher(s) should alert the Incident Room who will decide whether to evacuate the building(s). If nothing unusual is seen, the search should begin.

The search should be conducted methodically and systematically, moving in one direction around the area to be searched. It should be carried out in three sweeps:-

- **First Sweep** is to work around the edges of the room or bay, taking in the walls from top to bottom, and the floor area immediately beneath the wall. Look inside fireplaces, behind curtains and pelmets, behind and beside furniture around the edges of the room. The sweep should finish at the doorway where it began.
- **Second Sweep** should take in the furniture and the floor. Furniture should not be moved but drawers should be opened and searched, and gaps in and under furniture should be explored. If the floor covering shows signs of recent disturbance, it should be lifted.
- **Third Sweep** should cover the ceiling if it is of a kind in which objects might be concealed. Start at one corner and systematically search the whole surface.

After the search has been completed and if nothing has been found, the Incident Room should be informed immediately so that the area can be marked "clear" on the search plans.

NB: Searching should continue until the whole area has been cleared. Secondary devices are not unknown.

Use of Radios and Mobile Telephones

Until a suspect object is found the use of hand-held communications is often the only way of ensuring appropriate and speedy lifesaving procedures for search and evacuation. Once a suspect device has been located, those using hand-held communications should immediately move away and ensure that they and anyone else in the area move outside the cordon as quickly as possible.

If a Suspicious Object is Found, Follow the Golden Rules:-

- **DO NOT TOUCH OR MOVE IT.**
- If possible, leave a distinctive marker near (not touching) the device.
- Move away from the device to a designated control point, marking your route if possible.
- Inform the search team leader or the Incident Room.
- The Incident Room should implement the evacuation plan.
- Stay at the control point and draw an accurate plan of the location of the suspicious object.

The person finding the object should be immediately available for interview by the Police.

Evacuation Plan

Following discovery and confirmation of a suspect device, the Security Incident Team will instigate the evacuation procedure.

Size of Device	Distance of Cordon
Briefcase	100 metres
Saloon vehicle	200 metres
Large vehicle	Over 400 metres

The cordon must be controlled to prevent people from entering the danger zone.

Suspicious Packages

IF IN ANY DOUBT, EVACUATE THE AREA AND DIAL 999

Although terrorist or criminal incidents are extremely rare, staff should be alert to the risks of receiving harmful substances or explosive devices in the post.

The following practical steps should be taken to minimise the risks:-

- Open all mail with a letter opener.
- Open packages/envelopes with the minimum amount of movement.
- Do not blow into envelopes.
- Do not shake or pour out contents.
- Keep hands away from nose and mouth whilst opening mail.
- Wash hands after handling mail.

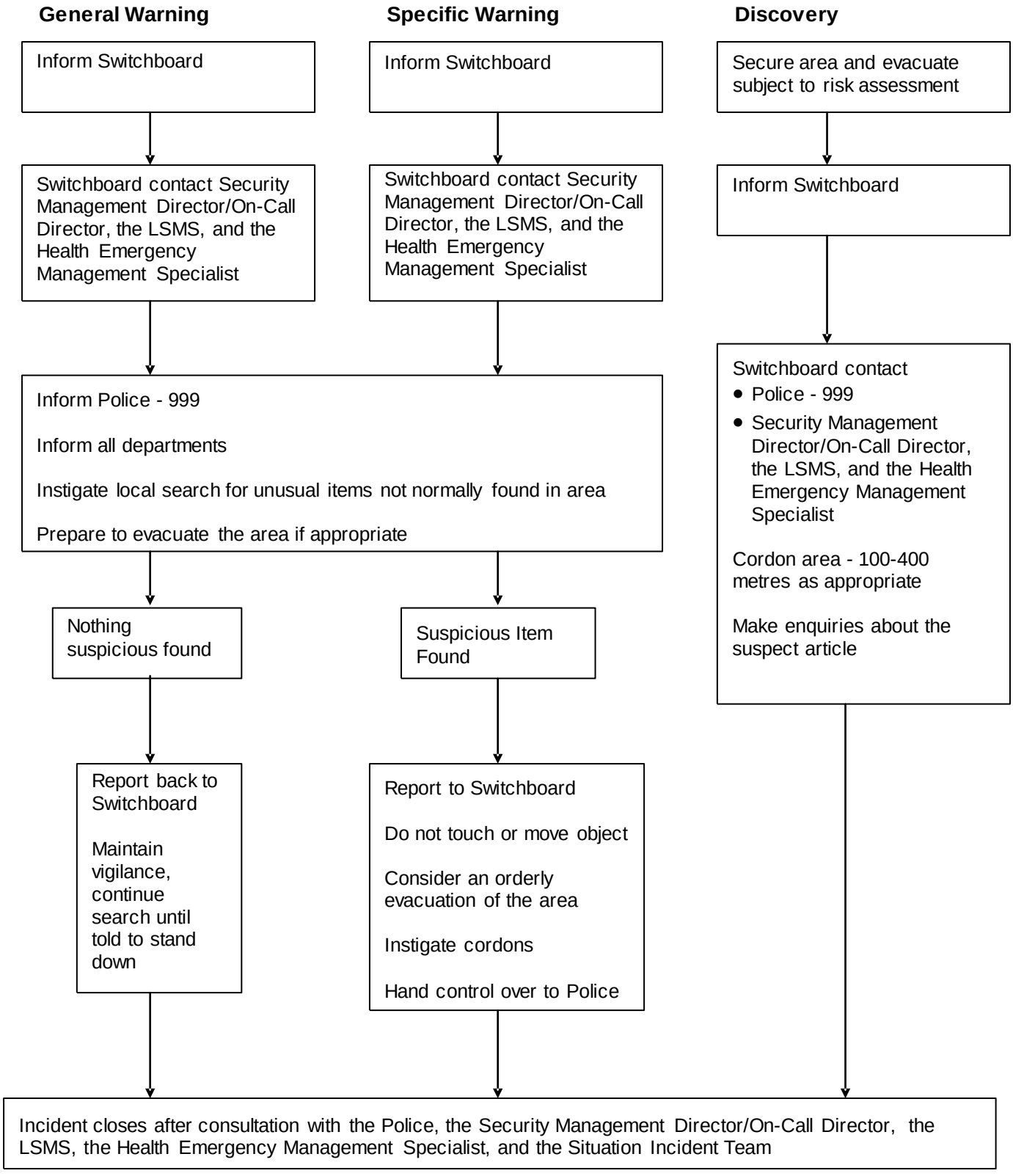
Some items that can trigger suspicion:-

- Discolouration, crystals on the surface, oily stains, strange odours, eg marzipan.
- Envelope with powder or powder-like residue.
- Excessive tape or string.
- Unusual size.
- Unusual weight for the size of the package.
- Lopsided or oddly-shaped parcel/envelope.
- Postmark that doesn't match the return address.
- Delivered by hand from an unknown source, or posted from an unexpected source.
- Excessive postage.
- Hand-written, block-printed, poorly addressed/misspellings of common words.
- No return address.
- Addressed to an individual no longer with the organisation.

If you are in any doubt about a package, DO NOT TOUCH IT, MOVE IT OR OPEN IT. Call the police on 999

Inform your Line manager or Building Manager and complete an incident report via Datix.

Incident Algorithm



n) Hostage Incidents

The Trust recognises the seriousness of any incident where it has been identified that a member of staff has been taken hostage during the course of their work either on Trust premises or any other associated property (eg community staff undertaking a home visit).

For the purposes of this Policy, a hostage situation is "*any situation where it has been identified that a person is being held against their will by force or threat of force (expressed or implied)".*

Whilst it is accepted that a hostage situation would in normal circumstances be easy to identify in a location where a number of staff routinely work (eg on a Ward or at a Health Centre), it would be difficult to identify that a hostage situation has arisen during a home visit or in premises where staff are working alone. For this reason it is the responsibility of all managers to ensure that robust lone working procedures are in place that identify the whereabouts of staff. If any member of staff (especially lone workers) has been identified as being "missing" during the course of their work and concerns have been raised about their safety then this fact should also be reported to the Police.

The following guidance is to be adopted, and should be included in the Security Protocol developed for each premises.

Contacting the Police

All hostage incidents are a matter for the Police and should be reported to them immediately by phoning 999.

The person reporting a hostage incident to the Police should make it perfectly clear that there is a hostage situation (suspected or actual) and give the following information where available:-

- The exact location of the incident, including known access/egress points.
- Details of the hostage taker, including their clinical condition and events leading up the incident.
- Details of hostage(s).
- A suitable rendezvous point for Police, where they will be met by appropriate personnel.
- Any known weapons or items being used (eg firearm or knife).
- Any known injuries to any party.

Once a hostage situation has been reported to the Police then it should also be reported to the LSMS, the Health Emergency Management Specialist, and the Security Management Director/On-Call Director. It will be the responsibility of one of these persons to ensure that the Chief Executive is informed and kept up-to-date with developments.

Before Police Arrival at the Scene

It will be the responsibility of the senior manager at the location to manage the situation in the first instance, and should be aware of, and adhere to, the following points:-

- No attempt should be made to enter into any form of discussion, unless failing to do so would place the hostage at immediate or greater risk.
- No negotiation should be undertaken and no requests granted.
- If confronted by the hostage taker(s) it must be stated that you do not have the authority to grant any of their demands.
- No intervention involving the use of force must be used unless:-
    - *Life is in immediate danger*
    - *Forcible intervention has a high probability of success*
- All non-essential staff and mobile patients should be withdrawn from the area, ensuring this is done without further aggravating the hostage situation.
- Arrangements should be made for all calls into the hostage area to be diverted if possible.

Following Police Arrival at the Scene

On arrival, the police will assume full command and control of the incident **WITHOUT EXCEPTION**.

The following Trust staff should be on hand to assist the police as appropriate:-

- Premises Manager/Estates Manager.
- On-call Director.
- LSMS.
- Health Emergency Management Specialist.
- Trust Communications Manager.
- Witness(es) to the incident.

Guidance for Staff (Hostage)

It is normal to feel frightened and powerless at the onset of a hostage situation, but it is important to try and remain as calm and rational as possible. The following guidance outlines what to do if you have been taken hostage.

- Do not say or do anything that may put you or others at risk.
- Do not lose hope and avoid an open display of despair.
- Initially, do not speak unless spoken to.
- If engaging in conversation, try to calm the hostage taker.
- Do exactly what you are told and do not make suggestions.
- Try to rest, but do not turn away from the hostage taker.
- If you need medication, calmly ask for it.

- Under no circumstances argue with the hostage taker.
- Remain observant throughout; you may be released or able to escape safely at any time.
- Expect noise and lights if a rescue attempt is made.
- In the case of a rescue attempt drop to the floor and stay there until told otherwise by the rescuers.

Post-Incident Management and Review

As soon as is practicable after the incident, a debrief must be convened between all parties involved to review the final outcomes, and to learn from any shortfalls in procedures.

Full support and guidance (including counselling via Occupational Health) will be afforded to all persons who have been unduly affected by any given incident.

o) Terrorism Incidents

NHS hospitals and healthcare premises are not normally the targets of terrorist activists; however, all staff should be constantly vigilant for the threat of terrorist activity.

Terrorist activities range from overt acts such as shootings, bombings and chemical attacks; they also take more subtle forms such as information gathering and blackmail.

Staff should be aware of suspect packages, unattended items, the threat of bomb attacks and suspicious incidents, which are to be reported in line with guidance published within this policy.

External advice from security specialists, including the Counter Terrorism Security Advisor (CTSA) employed by the West Mercia Police, will be obtained to ensure the provision of protective and counter- terrorism measures are appropriate to the threats posed to the Trust.

p) Security of Motor Vehicles and Bikes

All motor vehicles and bikes used by staff, visitors and other outside agencies should park in the authorised parking areas which have been provided and authorised by the Trust for this purpose.

The security of motor vehicles and bikes owned by staff or visitors is the responsibility of the owner. The Trust cannot accept liability for any motor vehicle, bike or any contents when they are parked on Trust sites.

Advice regarding keeping your vehicle Safe

The following list, are items which are included for the safe protection of motor vehicles and bikes:

- Lock it.
- Close windows.
- Do not leave property on view.
- Do not leave medicines/prescriptions or prescription pads on view.
- Do not advertise Doctor or Nurse-on-call unnecessarily.
- Remove Satellite navigation systems and dash cams.
- Secure Motorcycles with D lock or similar devices.
- Bikes should be secured to a bike stand, where available, with a good quality lock.

Any occurrences of theft, criminal damage or other offences in relation to vehicles should be reported immediately via the Datix Reporting System.

Where appropriate, Police should be contacted by the vehicle owner.

q) Site Access and Parking

Site Access

It should be noted, that Trust sites are private in relation to the entry and movement of vehicles. The Trust reserves the right to deny any vehicle access to a site, and to require drivers to conform to the designated traffic regulations and signs in order to ensure that:

- No obstruction is caused to fire exits.
- No obstruction is caused to loading and/or unloading areas, or the movement of patients, goods or the provisions of services.

Any person using vehicles of any description on the hospital site must comply with the Road Traffic Act 1991 regarding taxation, licensing, insurance, road worthiness and the reporting of accidents to the police.

Any person driving, or riding, a vehicle of any description on the hospital site and who causes an injury to a person or to property is required to report the matter to the Trust without delay as well as complying with the Road Traffic Act 1991 by notifying the police.

Parking

There are a limited number of drop off, pick up and disabled parking bays within the Trust sites for visitors and blue badge holders.

Parking is only authorised within the designated parking bays. Examples of areas where parking is not permitted are:

- Roads which are hatched by red or yellow lines.
- Roads which have double yellow lines.
- Disabled bays not displaying a valid blue badge.
- Ambulance or Patient transport bays.

Members of staff who ignore warnings regarding inappropriate parking whilst on Trust premises could be the subject of a report to their head of department which may result in disciplinary action being taken against them.

On some sites vehicle registration details may be captured by Parking Management Systems to facilitate access control and the issuing of parking charge notices for parking violations. Parking charges for parking infringements are not managed by the Trust, any appeals must follow the process noted on the parking charge notice.

r) Local Security Management Specialist Contact Details

Anyone who wishes to discuss issues relating to security management should speak to the Trust Local Security Management Specialist, details of which are given below:

- Name: Terry Feltus
- Telephone: • 01743 277635, or internal extension number 2274
  Email: terry.feltus@nhs.net
- Address: William Farr House, Mytton Oak Road, Shrewsbury, SY3 8XL