Doncaster and Bassetlaw Teaching Hospitals NHS Foundation Trust

Security Policy – Incorporating Bomb Threat/Suspect Packages

This procedural document supersedes: CORP/HSFS 15 v.7 Security Policy – Incorporating Bomb Threats/Suspect Packages

Did you print this document yourself?

The Trust discourages the retention of hard copies of policies and can only guarantee that the policy on the Trust website is the most up-to-date version. **If, for exceptional reasons, you need to print a policy off, it is only valid for 24 hours.**

Executive Sponsor(s):	Sam Wilde – Chief Finance Officer
Author/reviewer: (this version)	Kerry Williams Local Security Management Specialist (LSMS)
Date written/revised:	April 2025
Approved by:	Health and Safety Committee
Date of approval:	8th May 2025
Date issued:	5th June 2025
Next review date:	April 2028
Target audience:	All Trust Colleagues, Trust-wide

Amendment Form

Please record brief details of the changes made alongside the next version number. If the procedural document has been reviewed **without change**, this information will still need to be recorded although the version number will remain the same.

Version	Date Issued	Brief Summary of Changes	Author
Version 8	5th June 2025	• Change of the Executive Sponsor. • Expansion of Criminal acts by Trust colleagues. • Inclusion of security powers and self-search. • Expansion of GDPR for requesting door access reports for investigation. • Removal of Audit and Risk Committee (ARC). • Inclusion of Finance and Performance Committee (F&P). • Updated Appendix 1 - Procedure for Dealing with a Bomb Threat/Bomb threats checklist; included a link to the Hive, to complete the checklist electronically if required.	Kerry Williams
Version 7	March 2022	• Minor changes throughout. • Removal of Audit & Non-Clinical Risk Committee.	Kerry Williams
Version 6	4 October 2018	• Updated into new format. • Various minor changes and updates throughout the policy. • Removal of NHS Protect Guidance and Reference.	Kerry Williams
Version 5	April 2015	• Major changes made throughout, please read in full. • Updated into new format. • Bomb and Suspect Package Policy incorporated. • Security wearing body cameras.	Kerry Williams
Version 4	March 2012	• Duplicate references to other policies removed. • References to LSMS changed to Security Manager. • Equality Impact Assessment statement rationalised • Reference to Director of Estates and Facilities removed. • Duties of Chief Executive expanded. • Duties of Director of Finance rationalised. • Contact details of former LSMS removed.	David Clayton

Version 3	May 2010	• Updated in line with NHS Litigation Authority guidance. New Sections:
		  • Equality Impact Assessment
		  • Training
		  • Lockdown Procedures
		  • Associated Documents
		  • References
		• Policy now includes contact details of Local Security Management Specialist.
			Henry Grant

Contents

Page No.

1 INTRODUCTION

This policy document outlines how Doncaster and Bassetlaw Teaching Hospital NHS Foundation Trust will provide the best possible protection for its patients, staff, professionals and property. It is not acceptable for standards of patient care to be diminished by the actions of an irresponsible and anti-social minority.

The Trust will work to implement the strategies and procedures developed to create a safe and secure working environment. The Security strategy is intended to provide common goals, a clear business process to achieve them and a framework for all working in this area. The strategy puts into context the new approach to the management of security and outlines the new legal requirements that will apply to all NHS bodies in the NHS Standard Contract so that there can be guarantees that the highest possible professional standards are implemented.

2 PURPOSE

To protect the NHS so that it can better protect the public's health.

The priority aims for security in the Doncaster and Bassetlaw Hospital is to maintain perceived and actual:

- Personal safety of patients, staff and visitors.
- Security of personal property of patients, staff and visitors.
- Security of the Trust's property and buildings and assets.

This must be done in a way that balances with the overarching duty of providing comfortable, user-friendly, easily accessible services.

The protection of patients, staff and visitors will enable the continuation of our core activity, that is, the treatment and care of our patients to be conducted in a safe environment, free from worry or concern over the damaging effect that crime or the threat of violence gives. It will create an atmosphere of care and foster a better-motivated workforce. Additionally, the protection of assets, either corporate or personal will enable resources to be focused into patient care, rather than be diverted in the direct and consequential costs of losses incurred by criminal activity.

3 DUTIES AND RESPONSIBILITIES

3.1 Director of Infrastructure – Security Management Director (SMD)

- The Director of Infrastructure is the nominated Trust Security Management Director (SMD) and is responsible for the day-to-day function of security matters, a strategic overview and for specific site related matters.
- The SMD will be responsible for taking a lead and co-ordinating the approach and response to security issues within the Trust.
- The SMD will submit to the Chief Executive such reports and details of investigations as required.
- Bi-Annual reports will be submitted by the SMD and the Local Security Management Specialist (LSMS), to the Finance and Performance Committee (F&P) detailing security strategies and work plans. These will include the level of criminal activity, identify approved

Business Cases, monitoring arrangements of security procedures, details regarding training, police involvement and outcomes.

- The Director of Infrastructure Estates & Facilities has specific responsibility for ensuring that the Project Team liaises with, and seeks the specialist advice of, the LSMS to plan for security issues at the design stage of Capital Schemes.

3.2 Local Security Management Specialist (LSMS)

- Responsible for ensuring that there are appropriate management controls in place to ensure compliance, crime prevention and monitoring of security measures and procedures.
- Responsible for making such arrangements to identify potential security problems and to take corrective action as is necessary to enable the protection of staff, patients and visitors, property and assets.
- Responsible for ensuring compliance and monitoring of security measures and procedures.
- Will liaise with outside agencies such as the Home Office, Police, Prison Service, Probation Service, Counter Fraud, Crime Prevention Panel, Victim Support Units etc.
- Will be a point of reference, providing an operational security service to the Trust for the benefit of staff, visitors and patients.
- Develops a pro-active security culture among staff, professionals and patients to further raise awareness and encourage reporting.
- Takes a trust-wide approach to the identification and management of risks to prevent security incidents. This includes reviewing all locally undertaken risk assessments, monitoring progress with implementation and reporting trust-wide issues, trends and blocks to implementation.
- Ensures staff are equipped with the skills to resolve conflict.
- Delivers simple and consistent reporting systems, using clear and legally based decisions, enabling the detection of incidents.
- Works with other agencies to ensure a consistent approach is taken to accident investigation and violence; ensuring that staff and professionals are supported through the process.
- Ensures that the full range of sanctions is considered when dealing with offenders, that they are consistently applied, and provide good quality feedback to those who have suffered violence.
- To obtain redress where possible, and ensure that counselling and support is offered to staff.
- Works to ensure that health bodies work together so that action is consistent in minimising the impact of security issues on the NHS and the ability of staff and professionals to work effectively.
- To give advice and input in to all new schemes and developments across the Trust.

3.3 Divisional Director of Nursing

- To ensure that, as far as is reasonably practicable, security and the safety of patients, visitors and staff are reflected in all appropriate departmental policies and procedures.
- To ensure a yearly risk assessment of physical security and of other assets in their areas of responsibility is undertaken.
- The Trust risk assessment form, action plan template and risk assessment matrix are on the Trust intranet.

- The risk assessments and action plan are held locally for implementation. A copy of the risk assessment and plan is sent to the LSMS for monitoring of implementation and reporting to the Health and Safety Committee.
- To inform the LSMS of any changes within their Department/Ward that affects the security of the premises, following a risk assessment.
- To ensure that staff within their Department/Ward are instructed to allow only authorised persons to enter 'staff only' areas and, where it is safe to do so, challenge and prevent entry of all unauthorised persons. In circumstances where this action would put staff at risk, they should be instructed to call security to validate identity.
- To record details i.e. make, model, serial number etc., of all physical assets or otherwise important property within their Department/Ward and to ensure that these items where possible are secured and protected against theft or malicious damage.
- To keep a record of all keys issued to staff in their Department/Ward and reporting all losses of keys to the Security and Estates Departments.
- To ensure that arrangements are made to secure the Departments out of working hours and the safe custody of keys and to ensure that any security alarm or device to protect the property out of hours is set.
- To provide each employee with information, instruction and training as necessary to ensure the safety of themselves and others from the security risks associated with the activities they are employed to undertake.
- To ensure that staff are fully supported when making reports concerning fraud, violence, theft and damage or other security related incidents.
- To ensure that the Local Security Management Specialist is informed of all cases of theft or suspected theft of Trust property and details of any action taken. They will also inform the Local Counter Fraud Specialist immediately if fraud is suspected.

3.4 All Trust Colleagues

All colleagues are required to positively assist in the implementation of the Security Policy. All colleagues are responsible for compliance with the Security Policy, security procedures and arrangements.

It is vital that everyone recognises the need to maintain a high degree of vigilance and not prejudice their own safety, safety of patients, relatives, visitors and the security of property or assets due to acts of negligence or carelessness.

- To be responsible for promoting and maintaining security at all times by being involved in crime prevention and security measures, anticipating risks and taking action to remove, reduce or transfer them, and receive adequate training on these issues.
- To be aware of the security needs of the organisation and be familiar with the specific aspects of security policy and procedures which affect their own area of work.
- To report all incidents of criminal activity such as assaults, theft, and criminal damage including those incidents thought to be of a suspicious nature to their appropriate
- Supervisor/Manager and on the Trust incident reporting system, Datix, following the Trust Incident Reporting and Management Policy
- To be fully conversant with the methods and procedures for contacting Security staff.
- To report all incidents of suspected fraud to the LCFS or via the **NHS Fraud & Corruption.**
- Reporting line 0800 0284060. (online at www.reportnhsfraud.nhs.uk)

4 PROCEDURE

4.1 Legal Responsibilities

The Trust recognises its legal liability for Security. The role of the law regarding the security of the Trust premises is two-fold.

(a) It defines the Trust's duties and responsibilities to safeguard both its employees and those attending for treatment, and the consequences of failure to perform those duties sufficiently.
(b) It outlines the parameters within which the Trust can address its security needs and the action it can legally take to combat threats.

The relevant legislation is:

- Health and Safety at Work Act 1974
- Management of Health and Safety at Work Regulations 1999
- Police and Criminal Evidence Act 1984
- Children's Act 1989
- Unfair Contract Terms Act 1977
- Occupiers Liability Act 1984
- Mental Capacity Act 2005

The Occupiers Liability Act 1984 imposes a duty of care upon an occupier of premises to ensure that its visitors and their property are reasonably safe. The duty is more onerous in the case of children, since an Occupier must be prepared for children to be less careful than adults.

4.2 Criminal Acts by Trust Colleagues

The Trust may be liable if it fails to sufficiently protect patients and other Trust colleagues from the possibility of criminal acts by its employees.

The Trust is committed to maintaining high standards of integrity and accountability. Criminal acts by staff whether involving theft, fraud, assault or other offenses, undermine public trust and pose significant risks to patient safety, the Trust's reputation and overall operational effectiveness.

Definition of Criminal Acts

Criminal acts by NHS colleagues can include but not limited to:

- **Theft**: stealing NHS property, patient belongings, or medical equipment.
- **Fraud**: Misrepresentation for personal gain, such as falsifying timesheet, claiming unearned overtime or procurement fraud.
- **Violence or Assault**: Physical or verbal assaults on patients visitors or colleagues
- **Drug misuse or Theft**: Unauthorised possession or use of pharmaceuticals or controlled substances.
- **Data Breaches**: unlawful access, misuse, or sharing of confidential patient or Organisational data.

- **Misuse of Position**: Exploiting authority for personal gain, including bribery or inappropriate relationships with patients.

Legal Framework and NHS Standards

Relevant Legislation

- **Theft Act 1968**: Governs theft and related offenses
- **Fraud Act 2006**: Criminalises acts of deception for financial or personal gain.
- **Data Protection Act 2018**: Covers unauthorised data access of breaches.
- **Health & Safety at Work Act 1974**: Ensures safety for patient's staff and visitors.
- **NHS Counter Fraud Authority (NHSCFA):** Dedicated to identifying, investigating and preventing fraud within the NHS.
  Provides guidance to NHS Trusts on fraud prevention and handling.
- **Employment Law**: Aligns with disciplinary and dismissal processes under fair employment practices.

4.3 Risk Assessment

Risk Management is at the heart of the Security Strategy. Risk management techniques harness the information and experience of Trust staff (and external expertise if necessary); translating this into positive action to remove or manage hazards and reduce risks.

Risk assessment:

- Reviews the various activities of the Trust and identifies critical areas for the organisation.
- Identifies the risks that exist.
- What could go wrong?
- How could it happen?
- What would be the effect?
- Assesses those risks for potential frequency and severity.
- Eliminates the risks that can be eliminated.
- Identifies how remaining risks can be mitigated or managed.
- Develops and delivers a plan for implementing the identified changes.
- Provides current measurement and assists target setting for reduction in risks.

Departments will carry out appropriate risk assessment on physical security of premises and assets every year. This must be conducted by the department manager responsible for the area.

Any Security Risk Management Assessment featuring buildings, Department and external features of the Trust buildings will be carried out using the Home Office Crime Reduction Techniques.

These include the ten principles of Crime Prevention:

1. Target Hardening.
2. Target Removal.
3. Remove the Means to Commit Crime.
4. Reduce the Payoff (the gain from Crime).
5. Access Control.
6. Visibility/Surveillance.
7. Environmental Design.
8. Rule Setting.
9. Increase the Chance of Being Caught.
10. Deflecting Offenders.

Following a risk assessment on premises or assets, an action plan will be developed with timescales and nominated persons to carry out agreed action. The plan is kept by the Ward/Department manager.

If new premises or assets are commissioned within the Trust these will be risk assessed prior to operational use of them, in line with this policy.

The Department Manager is responsible for ensuring that suitable and sufficient Risk Assessments are completed for their own workplace in regards to security. The manager can delegate this task but ultimately they are responsible.

Further help and support with completing a security risk assessment is available from the Trust Health & Safety Advisor and LSMS. Training on The Principles of Risk Assessment is available via ESR and should be completed by all who complete risk assessments.

Copies of risk assessments and the action plan are sent to the LSMS for collation and review. The LSMS includes reports on trends and specific issues with implementation in their Bi-annual report.

4.4 Reporting Security Incidents

All security incidents and near misses must be reported on the Trust incident reporting system, Datix, following the Trust Incident Reporting and Management Policy.

These incidents are reviewed by the LSMS and investigated appropriately.

4.5 Access Controls

A Security Risk Management Assessment of access controls to Trust properties will be undertaken annually. The assessment will include:

- Physical Access
- Restricting Physical Access
- Security Equipment for Access Control
- Accessing Monitoring by Staff

For Net 2 access control measures please refer to the Trust Electronic Door Access Control Policy.

4.6 Identification

The Trust currently has a protocol in regard that all colleagues must display either a name badge or photographic ID card.

5 TRAINING/SUPPORT

Managers are responsible for ensuring all their Trust colleagues receive the type of initial and refresher training that is commensurate with their role(s).

Please note: The Standard Training Needs Analysis (TNA) – The training requirements of staff will be identified through a Departmental Risk Assessment for Violence & Aggression and a training needs analysis will be agreed. Role specific education will be delivered by the service lead.

Alternatively, training may be accessed via an approved e-learning platform where available. All Trust colleagues records are available on the Electronic Staff Record (ESR).

6 ASSET MANAGEMENT

In compliance with the NHS financial management regulations an asset register of items valued over £5,000 is maintained and complies with the organisations Standard Financial Instructions (CORP/FIN 1 B).

7 CONFLICT RESOLUTION

The Trust has a separate policy for Violence Prevention & Reduction (CORP/HSFS 5).

8 PREVENT POLICY

The aim of Prevent is to stop people becoming terrorists or supporting terrorism, protecting those who are vulnerable to exploitation from those who seek to get people to support or commit acts of violence. Prevent is part of the Governments Counter Terrorism Strategy. Further details can be found in the Trust Prevent Policy (CORP/RISK 25).

9 KEYS AND LOCKS

The following principles provide adequate control over keys with safety, and ensure accountability:

- It is the departmental managers responsibility to ensure that codes to any locking device i.e. digital/combination locks are only given to staff who require daily access to the department. It is recommended that the codes for these locks are changed frequently (every 3 to 6 months is recommended) this can be requested through the Estates helpdesk on 644111.
- Departmental keys should remain under the control of the department and should be accounted for in an orderly system.
- The keys to a department's main entrance must be accounted for at all times, either within the Department or at the point to which they are returned for safe custody when no longer required.
- There should be duplicates of all keys held in Estates.
- Duplicate, triplicate and any spare keys must be safeguarded and issues controlled.

- No extra keys should be cut to locks on departmental doors or the external doors to main buildings without the approval of the Departmental Manager and the Local Security Management Specialist respectively. Any unofficial key cutting may result in disciplinary action.

10 CCTV

- Comprehensive closed circuit television systems are in operation throughout the Trust. Separate Trust guidance has been produced which identifies the purpose, accountability, management and monitoring of the systems (CCTV Code of Practice).
- Security Guards wear Body Cams enabling all incidents to be recorded.
- Initially the use of these devices is a deterrent to an individual who may be of a mind-set of creating a conflict situation.
- All incidents are recorded and footage can be downloaded giving good quality images and evidence to be used in a court of law if required.
- CCTV complies with Closed Circuit Television Policy (CORP HSFS 34).

11 PROPERTY OF TRUST COLLEAGUES, VISITORS AND PATIENTS

If private property has been stolen, this needs to be reported through the internal Datix reporting system enabling the LSMS to carry out an investigation if required. It is the owner's and not the Trust's responsibility to report the matter to the Police.

Each Ward/Department must follow the Trust's procedure regarding the security of patient's personal property/monies during their stay in hospital. There is a separate policy for the handling of patient property (PAT/PA12 Patients' Property and Valuables).

The Trust does not accept liability for the loss of, or damage to, private property including motor vehicles or other modes of transport. The Trust will take all reasonable steps to safeguard vehicles but motor vehicles and other modes of transport brought onto Trust premises are done so entirely at the owner's risk.

Trust colleagues are advised to take adequate precautions to ensure the safety of their possessions and not bring valuables to work. Where a locker has been provided for personal use, the individual to whom it is allocated will be responsible for providing a suitable locking device.

Trust colleagues must report any loss or damage to their belongings and co-operate in any consequent enquiry into the loss or damage.

12 TRUST PROPERTY

It is an offence for colleagues to remove property belonging to the Trust without written authority. Failure to seek authority from line management could result in disciplinary action or criminal proceedings being taken. Trust colleagues must take all reasonable steps to safeguard Trust property whilst in their care. If theft or malicious damage to NHS property is suspected to have been committed, the Police will be informed.

13 SANCTIONS FOR THE SECURITY POLICY

Security incidents and breaches have a direct impact on the resources allocated to the NHS to deliver high quality patient care. Time and money spent on replacing stolen NHS equipment, repairing and replacing damaged NHS property or dealing with the consequence of violence is time and money diverted from the delivery of healthcare.

It is therefore important where security incidents and breaches cannot be deterred or prevented and a loss is incurred as a result, that the health bodies seek redress from those who are responsible, where this is appropriate.

Through professional investigative work carried out by the LSMS, health bodies will be able to identify resources lost as a result of security related incidents and breaches which can then form the basis for effective recovery.

Two principles lie behind effective recovery:

1. Monies lost through security-related incidents and breaches can be returned to patient care.
2. Recovery delivers an important deterrent message to staff, patients and the public that crime does not pay and that the NHS will always pursue redress from those who attack it and deprive it of valuable resources.

There are a number of avenues through which to seek redress:

- **Compensation through the criminal courts** – either as a sentence in its own right or in addition to another sentence imposed. The court may order a defendant to pay compensation to the victim(s) of their crime. Compensation orders are intended however to be used in straightforward cases where no great amount is at stake. They can be made in a number of cases, including (but not limited to) personal injury, loss and damage.

- **Civil action to obtain a civil remedy** - a civil remedy may be granted by a court to a party to a civil action. It may include (but not limited to) the common law remedy of damages (a sum of money awarded by a court to compensate a claimant for their losses) or an injunction (a remedy in form of a court order addressed to a particular person, that either prohibits them from doing or continuing to do a certain act or orders them to do a certain act).

- **Confiscation order** - an order that requires an offender convicted of an offence who has benefitted from that offence to pay a sum that the court considers appropriate. These are intended to be used in more complex and difficult cases where a substantial amount of money is at stake.

- **Investigation, compensation and redress** – The LSMS will, through investigation, seek the necessary information to allow health bodies to make a decision as to whether recovery of lost NHS resources and costs incurred should be pursued.
  These should include the costs of the investigation and of pursuing such action, where appropriate. The decision to pursue civil action should be made by the SMD based on the information supplied by the LSMS. Any such decision should take into account whether the chosen route is cost effective, i.e. ensure that the cost of recovery will not be larger than the amount lost.

- **Compensation** – Awarded by the criminal courts, compensation may not always cover the sums lost, the health body should consider civil action as a means of recovering the balance of the resources lost.

Security incidents and breaches have a direct impact on the resources allocated to the NHS to deliver high quality patient care. Time and money spent on replacing stolen NHS equipment, repairing and replacing damaged NHS property or dealing with the consequence of violence is time and money diverted from the delivery of healthcare.

It is therefore important where security incidents and breaches cannot be deterred or prevented and a loss is incurred as a result, that the health bodies seek redress from those who are responsible, where this is appropriate.

Through professional investigative work carried out by the LSMS, health bodies will be able to identify resources lost as a result of security related incidents and breaches which can then form the basis for effective recovery.

Two principles lie behind effective recovery:

- Monies lost through security-related incidents and breaches can be returned to patient care.
- Recovery delivers an important deterrent message to staff, patients and the public that crime does not pay and that the NHS will always pursue redress from those who attack it and deprive it of valuable resources.

There are a number of avenues through which to seek redress:

- **Compensation through the criminal courts** – either as a sentence in its own right or in addition to another sentence imposed. The court may order a defendant to pay compensation to the victim(s) of their crime. Compensation orders are intended however to be used in straightforward cases where no great amount is at stake. They can be made in a number of cases, including (but not limited to) personal injury, loss and damage.
- **Civil action to obtain a civil remedy** - a civil remedy may be granted by a court to a party to a civil action. It may include (but not limited to) the common law remedy of damages (a sum of money awarded by a court to compensate a claimant for their losses) or an injunction (a remedy in form of a court order addressed to a particular person, that either prohibits them from doing or continuing to do a certain act or orders them to do a certain act).
- **Confiscation order** - an order that requires an offender convicted of an offence who has benefitted from that offence to pay a sum that the court considers appropriate. These are intended to be used in more complex and difficult cases where a substantial amount of money is at stake.
- **Investigation, compensation and redress** – The LSMS will, through investigation, seek the necessary information to allow health bodies to make a decision as to whether recovery of lost NHS resources and costs incurred should be pursued.
- These should include the costs of the investigation and of pursuing such action, where appropriate. The decision to pursue civil action should be made by the SMD based on the information supplied by the LSMS. Any such decision should take into account whether the chosen route is cost effective, i.e. ensure that the cost of recovery will not be larger than the amount lost.

- **Compensation** – Awarded by the criminal courts, compensation may not always cover the sums lost, the health body should consider civil action as a means of recovering the balance of the resources lost.

14 DEALING WITH ILLICIT SUBSTANCES AND OFFENSIVE WEAPONS

If Trust colleagues identify or suspect that a patient or visitor has illicit substances or an offensive weapon they must call Security for advice.

Trust colleagues, including Security Officers, do not have the legal right to search patients or visitors. If a search is deemed necessary by staff or Security the police be called to undertake it.

15 SECURITY POWERS AND SELF SEARCH

Security do not have the legal right to search patients or visitors, it is recognised that security powers and self-search are critical tools used within Health Care Settings, particularly high risk areas like Emergency Departments.

Security powers must be utilised with care, balancing security needs with the dignity and rights of individuals. Clear polices, appropriate training and adherence to legal frameworks are essential to ensure these practices are justified, proportionate and effective.

Self – Search: Overview and Purpose

Self – search is a process in which individuals e.g., patients, staff or visitors are asked to check their belongings or outer clothing in the presence of a Security Officer or authorised member of staff. It aims to:

- Prevent the introduction of prohibited items (e.g., weapons, drugs or alcohol).
- Deter theft or unauthorised removal of NHS property.
- Ensure compliance with the Trust or ward expectations.

Security Powers: Scope and Application

NHS security powers are exercised within the limit of the law and include:

- **Self-search**: Encouraging individuals to cooperate by inspecting their belonging themselves
- **Prohibited item seizure**: Confiscation of items deemed a security threat or against Trust policy.

16 INVENTORIES AND SECURITY MARKING OF VALUABLE EQUIPMENT

Ward and Department Managers will ensure that an inventory is maintained of all the ward and department equipment. The inventory will be based upon, but not restricted to, those items identified as belonging to the ward or department upon the Trust's asset register.

Valuable and/or attractive items of equipment should be marked by individual departments to deter theft and assist in identification in the event of loss or theft. It is the departmental manager's responsibility to ensure the equipment is marked and a log kept. The LSMS can advise on suitable marking equipment.

17 BOMB THREAT/SUSPECT PACKAGES

Bombs or 'improvised explosive devices' may be used by those wishing to cause fear, economic loss, disruption or personal injury. Bombs themselves may fall into one or more of the following types: explosives, fragmentation, incendiary, chemical, biological, radiological and nuclear.

While the risk of an individual being caught up in a bomb-related incident is low, each health body has a responsibility under The Management of Health and Safety at Work Regulations 1999 to minimise that risk.

Hoax bomb threats are an everyday occurrence and can greatly reduce a health body's ability to deliver healthcare. They can cause a great deal of upset and, in some cases, fear amongst staff, patients and visitors. They also have a financial impact on health bodies in terms of reduced productivity, cancelled operations and appointments, and so on. Any bomb or similar hoax must be reported to the police, if they are not already involved. LSMS should act as the point of contact with the police, to support their investigation and provide any evidence that may assist with this, including information to support a request for compensation from those responsible. LSMS should monitor progress and also consider the possibility of seeking civil redress for any loss of resources or costs incurred by the health body as a consequence of the incident.

Bomb threats are a matter for the police, who must be called using the 999 emergency service as soon as possible. The staff member making this call should make it clear that a suspect device has been located or that a bomb threat has been received. The person who finds the suspect device or receives a bomb threat should be made available for interview by police or other authority expert.

Each telephone threat, written message or other means of communication alleging that a bomb has been or will be placed must be considered serious and should immediately be investigated.

A checklist for Trust colleagues receiving a telephone bomb threat, (see Appendix 1).

The procedure for Trust colleagues encountering a suspect package, (see Appendix 2).

18 FRAUD

Fraud which includes bribery and corruption is a serious offence and diverts Trust funds away from patient care. All allegations of fraud are taken seriously by the Trust and offenders face a range of sanctions, which include criminal, civil and disciplinary action.

Staff suspecting fraud should report their concerns to the Local Counter Fraud Specialist (LCFS) within the Trust or make a referral to the NHS Fraud and Corruption Reporting Line on 0800 0284060 (or online at www.reportnhsfraud.nhs.uk) Refer to the Fraud Bribery & Corruption Policy and Response Plan for further details.

19 PURCHASE OF SECURITY SYSTEMS

Divisions / Departments must consult the Local Security Management Specialist and the Estates Department before purchasing security equipment or systems (such as automated access control systems, including video/intercom systems and swipe card readers, CCTV, security lighting and intruder alarms). This is to ensure compatibility of the system with existing systems and compliance with other statutory regulations and guidance.

All new build and refurbishment elements should comply with 'Secured by Design' which is a crime prevention initiative managed by ACPO CPI Limited on behalf of the UK Association of Chief Police Officers. This work must also comply with the Trust's specification for security installations on new build and refurbishment works.

20 RELATIONSHIPS WITH THE POLICE

It is the Trust's policy to maintain a professional working relationship with the Police to our mutual benefit.

Regular liaison takes place between the Local Security Management Specialist and the local Police command.

Liaison between the Local Security Management Specialist and Police departments will take place to action specific matters.

Police will be given adequate facilities and proper assistance for the conduct of any investigation on Trust property. The Chief Executive or Nominated Manager will have regard for the disruption of patient care and Trust legal responsibilities regarding the confidentiality of information.

21 LOCKDOWN

Lockdown is the process of controlling the movement and access – both entry and exit – of people (NHS colleagues, patients and visitors) around a trust site or other specific trust building/area in response to an identified risk, threat or hazard that might impact upon the 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 security personnel.

The Trust undertakes lockdown testing and a Risk Profile for the site. This is reviewed every three years or after:

- Any incident requiring a lockdown.
- As part of any new build.
- As part of the review of the Major Incident Plan (MIP).
- Any change in legislation whichever is sooner.

22 MONITORING COMPLIANCE WITH THE PROCEDURAL DOCUMENT

The LSMS reviews all risk assessments and all incidents relating to security of premises and assets and reports quarterly to the Health and Safety Committee on:

- Risk assessments
- Trends
- Progress with action plans
- Blocks to implementation
- Incidents
- Progress with action plans

The Health and Safety Committee will ensure implementation plans are completed.

What is being Monitored	Who will carry out the Monitoring	How often	How Reviewed/ Where Reported to
Risk Assessments	LSMS & Health & Safety Advisor	As required	As required
Trends	LSMS	Quarterly	Reports to Trust Health & Safety Committee and Audit & Risk Committee
Incidents	LSMS & Health & Safety Advisor	Weekly	As above
Progress with action plans	LSMS & Health & Safety Advisor	As Required	Departmental Managers and Trust Health & Safety Committee

23 DEFINITIONS

LSMS - Local Security Management Specialist.

Non-physical assault – 'the use of inappropriate words or behaviour causing distress and/or constituting harassment', this includes:

- Offensive language, verbal abuse and swearing, which prevents staff from doing their job or makes them feel unsafe.
- Loud and intrusive conversation.
- Unwanted or abusive remarks.
- Negative, malicious or stereotypical comments.
- Invasion of personal space.
- Brandishing of objects or weapons.
- Unsuccessful physical assaults.
- Offensive gestures.
- Bullying, victimisation or intimidation.
- Threats or risk of serious injury to a member of staff, fellow patients/clients or visitors.
- Stalking.
- Spitting.
- Alcohol or drug fuelled abuse.
- Unreasonable behaviour and non-cooperation such as repeated disregard of hospital visiting hours.
- Any of the above linked to destruction of or damage to property.

Physical assault - 'the intentional application of force to the person of another, without lawful justification, resulting in physical injury or personal discomfort.'
SMD – Security Management Director.

24 EQUALITY IMPACT ASSESSMENT

The Trust aims to design and implement services, policies and measures that meet the diverse needs of our service, population and workforce, ensuring that none are disadvantaged over others. Our objectives and responsibilities relating to equality and diversity are outlined within our equality schemes. When considering the needs and assessing the impact of a procedural document any discriminatory factors must be identified.

An Equality Impact Assessment (EIA) has been conducted on this procedural document in line with the principles of the Equality Analysis Policy (CORP/EMP 27) and the Equality Diversity and Inclusion Policy (CORP/EMP 59).

The purpose of the EIA is to minimise and if possible remove any disproportionate impact on employees on the grounds of race, sex, disability, age, sexual orientation or religious belief. No detriment was identified. (See Appendix 3)

25 ASSOCIATED TRUST PROCEDURAL DOCUMENTS

Incident Management Policy - CORP/RISK 33
Reporting and Management of Incidents and Near Misses - CORP/RISK 13
IMT Security Policy - CORP/ICT 2
Confidentiality Code of Conduct - CORP/ICT 10
Missing Patient Policy - PAT/PS 1
Serious Incidents (SI) Policy - CORP/RISK 15
Violence Prevention & Reduction Policy – CORP/HSFS 5
Lone Workers Policy - CORP/HSFS 3
Fire Policy - CORP/HSFS 14
Arrangements for the Provision of Care to Individuals who are Violent or Abusive (Age 18 or over) - PAT/PA 6
Patients' Property and Valuables - PAT/PA 12
Fraud Bribery & Corruption policy and Response Plan - CORP/FIN 1D
Abduction policy - PAT/PS 19
Prevent Policy - CORP/RISK 25
Risk identification, Assessment & Management Policy - CORP/RISK 30
Equality Diversity and Inclusion Policy - CORP/EMP 59
Closed Circuit Television Policy CORP/ HSFS 34

26 DATA PROTECTION

Any personal data processing associated with this policy will be carried out under 'Current data protection legislation' as in the Data Protection Act 2018 and the UK General Data Protection Regulation (GDPR) 2021.

Under the General Data Protection Regulation (GDPR), accessing an individual's entry and exit data must be conducted lawfully, fairly and transparently. Such data should only be accessed when necessary and proportionate for specific purposes, such as identifying crime, fraud or Health and safety concerns.

Any request for this data must be made to the Trust Local Security Management Specialist (LSMS) and must be justified under a legal basis, such as legitimate interests ensuring that the information is used strictly for the intended investigation.

For further information on data processing carried out by the trust, please refer to our Privacy Notices and other information which you can find on the trust website: https://www.dbth.nhs.uk/about-us/our-publications/information-governance/

27 REFERENCES

- Health and Safety at Work Act 1974
- Secretary of State Directions Nov 2003 Violence Against Staff
- Management of Health and Safety at Work Regulations 1999
- Police and Criminal Evidence Act 1984
- Children's Act 1989
- Unfair Contract Terms Act 1977
- Occupiers Liability Act 1957
- Occupiers Liability Act 1984
- Health Service circular 1999/226 'Campaign to stop violence against staff working in
- the NHS: Zero Tolerance'
- Health Service circular 1999/229 'Working together securing a quality workforce for The NHS: Managing violence, accidents and sickness absence in the NHS'.
- CFSMS 'Tackling violence against NHS staff' November 2003
- CFSMS 'A framework for reporting and dealing with non-physical assaults against NHS staff and professionals' 2004

APPENDIX 1 – PROCEDURE FOR DEALING WITH A BOMB THREAT

In all cases where a bomb threat is received, the police should be informed immediately and kept advised as to what action is being taken.

Switchboard operators most frequently have to deal with telephone bomb warnings; however, any member of staff may be confronted by such a message.

Bomb Threats Checklist

To complete this form electronically, please see link to this form on the Hive…
>>> https://extranet.dbth.nhs.uk/document/2025-02-28_bomb-threats-checklist/

ACTIONS TO BE TAKEN ON RECEIPT OF A BOMB THREAT

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

ASK THESE QUESTIONS AND RECORD ANSWERS AS ACCURATELY AS POSSIBLE:

1. Where exactly is the bomb right now?	7. What is your name?
2. When is it going to explode?	8. What is your address?
3. What does it look like?	9. What is your telephone number?
4. What does the bomb contain?	10. Do you represent a group or are you acting alone?
5. How will it be detonated?	11. Why have you placed the bomb?

6. Did you place the bomb? If not you, who did?	12. Record time completed:

INFORM SECURITY OR COORDINATING MANAGER

DIAL 999 AND INFORM POLICE

Name and telephone number of person informed:	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 ☐ Age

Nationality

Threat language:

☐ Well spoken ☐ Irrational ☐ Taped
☐ Foul ☐ Incoherent

Caller's voice:

☐ Calm	☐ Slurred	☐ Lisp	Familiar (if so, who did it sound like?)
☐ Crying	☐ Excited	☐ Rapid	
☐ Clearing throat	☐ Stutter	☐ Deep	Accent (If so what accent?)
☐ Angry	☐ Disguised	☐ Laughter	
☐ Nasal	☐ Slow	☐ Hoarse	

Other (please specify)

Other sounds:

☐ Street noises	☐ Motor	☐ PA system	☐ Office machinery
☐ House noises	☐ Clear	☐ Booth	Other (please specify)
☐ Animal noises	☐ Voice	☐ Music	
☐ Crockery	☐ Static	☐ Factory machinery	

Remarks

Additional notes

Signature:	
Print name:	
Date:	

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

1. Do not reply to, forward or delete the message
2. If sent via email, note the address
3. If sent via social media, what application has been used and what is the username/ID?
4. Dial 999 and follow police guidance

5 Preserve all web log files for your organisation to help the police investigation (as a guide, 7 days prior to the threat message and 48 hours after)

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

Retention period: 7 years

APPENDIX 2 – PROCEDURE FOR DEALING WITH A SUSPECT PACKAGE

- Immediately contact the most senior person available or the Senior Manager/Director on call.
- **DO NOT HANDLE** any suspect package.
- If you are especially worried, then evacuate the area and await the arrival of the Police/Senior Manager.

APPENDIX 3 - EQUALITY IMPACT ASSESSMENT PART 1 INITIAL SCREENING

~~Service/Function~~/Policy/~~Project/Strategy~~	Division	Assessor (s)	New or Existing Service or Policy?	Date of Assessment
Security Policy-– Incorporating Bomb Threat/Suspect Packages	Estates & Facilities	Kerry Williams	Existing	April 2025

1) Who is responsible for this policy? Name of Division/Directorate: Estates & Facilities

2) Describe the purpose of the service / function / policy / project/ strategy? Providing a safe & Secure Environment for Trust Colleagues & Patients

3) Are there any associated objectives? Legislation, targets national expectation, standards: N/A

4) What factors contribute or detract from achieving intended outcomes? – N/A

5) Does the policy have an impact in terms of age, race, disability, gender, gender reassignment, sexual orientation, marriage/civil partnership, maternity/pregnancy and religion/belief? Details: [see Equality Impact Assessment Guidance] - No

- **If yes, please describe current or planned activities to address the impact** [e.g. Monitoring, consultation] – N/A

6) Is there any scope for new measures which would promote equality? [any actions to be taken] N/A

7) Are any of the following groups adversely affected by the policy?

Protected Characteristics	Affected?	Impact
a) Age	No	
b) Disability	No	
c) Gender	No	
d) Gender Reassignment	No	
e) Marriage/Civil Partnership	No	
f) Maternity/Pregnancy	No	
g) Race	No	
h) Religion/Belief	No	
i) Sexual Orientation	No	

8) Provide the Equality Rating of the service / function /policy / project / strategy – tick (✓) outcome box

Outcome 1 ✓	Outcome 2	Outcome 3	Outcome 4

If you have rated the policy as having an outcome of 2, 3 or 4, it is necessary to carry out a detailed assessment and complete a* **Detailed Equality Analysis form – see CORP/EMP 27.

Date for next review: April 2028

Checked by: Sean Tyler – Head of Compliance **Date:** April 2025