University Hospitals of Leicester NHS
NHS Trust

Security Policy

Approved By:	**Trust Board**
Date Approved:	**25 July 2002**
Trust Reference:	**B32/2024** **This version replaces the old cat A, Trust Ref: A14/2002. PGC is aware of the Trust Board's decision. Agreed 11th April 2024.**
Version:	**5**
Supersedes:	**4 – December 2016**
Author / Originator(s):	**Vincent Smith & Simon Daley.** **Local Security Management Specialists**
Name of Responsible Committee/Individual:	**Security Management and Police Liaison Group** **Medical Director**
Latest Review Date	**17 December 2021 – Policy and Guideline Committee**
Next Review Date:	**April 2025**

CONTENTS

Review date and Details of changes made during review:

Director of Quality Governance replaces Director of Safety and Risk

Section 6: Security Strategy is a new section that specifically details the requirements for Security Management in relation to new builds and major refurbishments.

KEY WORDS

Security, Police, Crime Prevention, Local Security Management Specialist (LSMS), Lockdown, Fraud

1 INTRODUCTION

1.1 This document sets out the University Hospitals of Leicester (UHL) NHS Trust's policy for security. The University Hospitals of Leicester NHS Trust is committed to delivering a safe environment for the provision of high quality health care, and the protection of staff, patients and visitors and their property, as well as that of the Trust. This document outlines the key elements of the Trust's approach to achieve this objective.

It is essential that all security incidents are reported to the Security Department at the relevant site, as follows: LRI ext. 1 6767; GH ext. 1 2999; LGH ext. 14292.

SUMMARY

The Health and Safety at Work etc Act 1974, the Management of Health and Safety at Work Regulations and the Secretary of State Directions for the management of security places duties on employers and employees. This document sets out the University Hospitals of Leicester (UHL) Trust Policy and procedures for the management of security.

2 POLICY AIMS

The aim of this policy is to set out how the Trust manages security. The Trust Board is committed to providing a secure environment for the delivery of quality health care. With respect to security management, the Trust will ensure measures are in place to implement the Secretary of State directions by:

2.1 Conformity with the Care Quality Commission and NHS England.

2.2 Clearly defined roles andresponsibilities.

2.3 The protection of Trust and personal property against theft, fraud and damage.

2.4 The physical security of confidential information. (Information Governance).

2.5 The completion of Risk Assessments and completion of a risk register.

2.6 The creation of local security procedures and departmental policy.

2.7 The harmonisation of security provision across the UHL.

2.8 The promotion of crime prevention awareness amongst staff and other site users.

3 Policy Scope

3.1 This Policy applies to all UHL staff including bank, temporary, agency and volunteer staff and contractors employed by the Trust and extends to all tasks undertaken.

3.2 This policy does not cover information security as this is covered by the Information Security Policy

4 Definitions

LSMS	The person appointed to undertake the duties of an accredited Local Security Management Specialist in accordance with Secretary of State Directions to health bodies on measures to tackle violence and general security management measures and any subsequent advice or guidance issued by NHS England.

5 Roles and Responsibilities

The UHL Health and Safety Policy sets out the roles and responsibilities for all staff. Additional responsibilities to enable effective security management are detailed below:

5.1 Trust Board :-

The Medical Director, on behalf of the Chief Executive, is the designated Security Management Director, who has specific responsibility for all security issues across the Trust, with the exception of fraud and corruption, which is the responsibility of the Chief Financial Officer.

5.2 The Security Management Director shall be responsible for overseeing:-

5.2.1 The work of the Local Security Management Specialist (LSMS).

5.2.2 The implementation and updating of the Security Policy.

5.2.3 The development of the Security Strategy.

5.2.4 Liaising with local Police and other agencies.

5.2.5 Care Quality Commission and NHS England standards relating to security.

5.2.6 Work to reduce violence and aggression to staff and patients.

5.3 Director of Quality Governance

5.3.1 Act on the instructions of the Security Management Director.

5.3.2 Chair the Security Management and Police Liaison Group meetings.

5.4 Security Management and Police Liaison Committee. The Security Management and Police Liaison Group (SM PL C) is a multi-disciplinary group chaired by the Director of Quality Governance. The Group shall be responsible for the formation and implementation of the Security Policy, monitoring performance and the organisational overview of risk.

5.5 The Local Security Management Specialist (LSMS) can be contacted through the corporate Health and Safety Services or via Mobile-07961294301 or Mobile-07946328148

The LSMS shall be responsible for:-

5.5.1 Developing and implementing the Trust's reduction of Violence and Aggression Strategy.

5.5.2 Developing and implementing the Trust's Security Policy.

5.5.3 Working with and reporting to NHS England in accordance with Secretary of State Directions for violence reduction standards.

5.5.4 Fulfilling the duties of the LSMS in relation to violent and aggressive incidents, as described in the Management of Violence, Aggression and Disruptive Behaviour Policy on INsite.

5.5.5 Investigation of security incidents and suspected security breaches, liaising with the Security Manager as necessary.

5.5.6 Liaison with local Police and other agencies.

5.5.7 In conjunction with the Trust's Emergency Planning Officer, liaise with East Midlands Counter Terrorist Security Advisor and assist with the development of an incident plan.

5.5.8 Attending the University Hospitals of Leicester NHS Trust Security Management and Police Liaison Committee meetings.

5.5.9 Reporting to the University Hospitals of Leicester NHS Trust Security Management and Police Liaison Committee.

5.5.10 Writing an annual report and annual LSMS work plan.

5.5.11 Reviewing the should be: Management of Violence, Aggression and Disruptive Behaviour Policy [including restraint guidance] – B11/2005, to reflect changes in legislation, guidance and best practice.

5.5.12 Acting as lead for NHS England standards relating to security and the reduction of violence standards.

5.5.13 Attending such meetings and training as deemed necessary to maintain the LSMS accreditation.

5.5.14 In conjunction with the security managers, assist wards and departments with security initiatives, risk assessments and risk mitigation strategies.

5.6 Director of Estates & Facilities :-

The Director of Estates & Facilities shall be responsible for:-

5.6.1 The development of local security procedures and the implementation of Trust policy.

5.6.2 The provision of a suitably staffed security service at each of the Hospitals.

5.6.3 Ensuring that there is a suitably equipped security control room present at the Leicester Royal Infirmary, Glenfield Hospital and the Leicester General Hospital.

5.6.4 Ensuring that sufficient funding is available for the installation / maintenance / upkeep of all physical security assets, including CCTV and Body worn cameras.

5.7 Security Manager:-

UHL has a manager designated with responsibility for the local security function. This manager's duties under this policy include:-

5.7.1 Be responsible for the management of the local security team, and ensure they work within this Policy.

5.7.2 Be responsible for ensuring that security staff respond to incidents / requests for assistance / reports of crime in a prompt and appropriate manner.

5.7.3 Be an active member of the Security Management and Police Liaison Group.

5.7.4 Work with and support the work of the Local Security Management Specialist with the investigation of security incidents, suspected security breaches and/or on security initiatives.

5.7.5 Be responsible for implementing site lockdown procedures as and when required. .

5.8 Clinical Directors/Heads of Nursing :-

Clinical Directors and Heads of Nursing must take accountability for the CMGs for which they are responsible. This will include, but not limited to:-

5.8.1 Ensuring that individual managers and staff are aware of their responsibilities.

5.8.2 Promoting security awareness through education and training.

5.8.3 Ensuring that departmental security policies are produced where appropriate.

5.8.4 Co-ordinating a programme of risk assessments covering all areas where appropriate.

5.8.5 Ensuring a training needs analysis is completed identified through risk assessment.

5.8.6 Assisting the LSMS in any investigation relating to their area of responsibility.

5.9 Wards/Departments/Local Managers:-

Shall be responsible for the following in relation to the area for which they have management responsibility :-

5.9.1 Carrying out Security Risk Assessments as detailed in section 6.2

5.9.2 Developing and implementing local Security Policy and Procedures, commensurate with identified risk.

5.9.3 Creating and maintaining a security culture within the department.

5.9.4 Ensuring training needs are identified and met (see Section 6).

5.9.5 Ensuring that this Policy is implemented.

5.9.6 Assisting the LSMS in any investigation relating to their area of responsibility.

5.10 All Staff :-

Everyone working within the Trust has a responsibility to :-

5.10.1 Be vigilant at all times, reporting anything suspicious as soon as possible to their line manager and the Security team responsible for their site.

5.10.2 Act within the policies and procedures laid down by the Trust, both at a local and corporate level.

5.10.3 Wear photo identification badges at all times whilst on duty, ensuring that they are clearly visible.

5.10.4 Act on the concerns of patients and visitors in relation to security matters.

5.10.5 Raise any concern they may have regarding security with their line manager and/or the LSMS including the Trust safeguarding team and the police.

5.10.6 Co-operate with any investigation into security incidents or suspected security breaches.

5.10.7 Attend training as identified in Section 7.

5.10.8 Report all incidents of violence, aggression, unacceptable behaviour, lost / missing / stolen items on Datixweb.

6. Security Management Strategy

6.1 The overriding principle for the security strategy of UHL is to support the provision of high quality healthcare through a safe and secure environment that protects patients, staff and visitors, their property and the physical assets of the organisation.

6.2 This will be achieved through a combination of proactive security patrols, engagement and security awareness of staff and the use of physical security and surveillance capabilities. It is informed a by a number of established guidelines and documents that detail specific considerations i in relation to security matters.

6.3 "Secured by Design" (SBD) is the official police security initiative that works to improve the security of buildings and their immediate surroundings to provide safe places to live, work, shop and visit. Principles shall by applied to all new developments and alterations to existing buildings. It shall be the responsibility of the scheme project manager and design team to ensure these principles are applied, and where practical and cost effective, are implemented within the cost envelope of the scheme.

6.3.1 The scheme project manager must involve the LSMS and Security Manager to seek their professional views on all security related matters relating to new developments and/or alterations to existing buildings.

6.3.2 Design teams should consult with the Crime Prevention Design Adviser of Leicestershire Police in conjuction with, and via the Trust LSMS.

6.3.3 As a principle the following Trust requirements should be included in the design.

6.3.4 Continuity of CCTV coverage of public receptions and corridors in the building. This is limited to the public circulation spaces of building and does not include departmental corridors unless there are specific security requirements for this such as counter terrorism.

6.3.5 CCTV must link to the trust control room for each hopsital site

6.3.6 The external perimeter of any new build must be covered by CCTV (using existing or new installation of cameras)

6.3.7 An ability to lock down builds when required via the Trust Lockdown Policy

6.3.8 Security of assets through the use of access control and alarm systems

6.3.9 The appropriate use of access control systems to prevent unauthorised access and in some cases egress to and from departments

6.4 Meeting the requirement of legislation relating to the security of biological and radioactive materials which could be used for terrorist purposes. Particular considertaion should be given to the measures that aim to;

- To Deter a would-be terrorist – by providing physical and electronic security measures, coupled with good management practices;
- Detect an intrusion – by providing alarm and visual detection systems with verification;
- Delay an intrusion for a sufficient period of time to allow a response force to attend - by putting in place physical security measures. (Counter Terrorism Specialist Advice) Contacts available through the Local Security Management Specialists).

6.5 All new design should meet the principles laid down in the "Crowded Places Guidance. Nov. 2020. Published by the National Counter Terrorism Security Office."

7 Policy Statements, Standards, Procedures, Processes and Associated Documents

7.1 Local Security Policy / Procedure

Security policies operate at two levels. The first is this hospital wide policy, and this sets out a broad approach to security on a hospital wide basis and, specifically, identifies individuals' responsibilities.

The second is at a local level. Whilst it will not be necessary in all areas, further additional measures should be considered by CMG 's . This will particularly be the case in areas that have high value or critical assets or where the nature of the work involves particularly vulnerable staff or patients. Support and advice in developing local policies and procedures is available from the LSMS.

Guidance on content of such local policies/procedures is listed below:

7.1.1 Clear statement of the objectives of the policy.

7.1.2 Reference to this policy.

7.1.3 What to do if there is an incident/incident reporting.

7.1.4 Reference to the staff handbook on INsite.

7.1.5 Key responsibilities of all individuals within the ward/department.

7.1.6 Key risk areas (these will be identified following a risk assessment).

7.1.7 Personal property.

7.1.8 Training.

7.1.9 Other specific issues, e.g. key management, departmental lock up, etc.

7.1.10 Wearing of photo ID badges.

7.1.11 Personal safety.

7.1.12 Any relevant information specific to a ward/department/building.

7.1.13 Local policies will be approved at CMG Boards.

7.2 Risk Assessments

7.2.1 Where it is considered that a security risk exists relating to premises or assets, a risk assessment should be carried out unless otherwise agreed in consultation with the LSMS.

7.2.2 Risk assessments should be carried out by wards/departments, and wherever possible risk should be eliminated. If this cannot be achieved, then systems and procedures should be put into place to minimise any risk. Where the need for capital investment is identified, CMG's shall be responsible for presentation of business cases to the Capital Monitoring and Investment Committee. The management of risks identified must be in line with UHL's Risk Management Policy.

7.2.3 Support and guidance in the development of risk assessments is available from the LSMS.

7.2.4 Action to mitigate risks will be monitored on a regular basis to ensure implementation. The frequency of monitoring is determined by the severity of the risk and will be performed at a local level for all risks. In addition, actions associated with high and extreme risks will also be monitored at B oar d meetings on a monthly basis. The UHL Risk Management Policy provides details of risk monitoring / review frequencies and the reporting process.

7.2.5 The Security Management and Police Liaison Group shall maintain an overview of the security risk profile by monitoring the Trust's risk register.

7.3 Lockdown Procedures

7.3.1 From time to time, in response to a variety of incidents, it may be necessary to lockdown part of, or the whole of, the site.

7.3.2 The Trust has lockdown procedures relating to each site and specific high risk areas. Details of the arrangements for this are contained in the document entitled 'UHL Lockdown Plan', available on INsite.

7.3.3 The Security Management and Police Liaison Group will evaluate the lockdown areas on an annual basis.

7.3.4 All staff are responsible for notifying the LSMS and Security Manager of any significant material changes that may impact on the lockdown procedure. The LSMS / Security Manager will in turn inform the Emergency Planning Officer, so that these can be taken into consideration and reviewed accordingly.

7.3.5 The CMG's are responsible for informing the LSMS and the Security manager of any changes in the security risk profile of their area. For example, after the installation of high value equipment or the new use/storage of radioactive materials.

7.4 Identification Badges & Name Badges

7.4.1 The Trust provides photo ID Badges for all staff, including bank and agency staff. These must be worn at all times whilst staff are on duty and should be clearly visible. Managers shall be responsible for ensuring compliance.

7.4.2 Managers are responsible for ensuring that all ID badges and name badges laptops, IPads and keys are recovered from staff leaving the organisation. ID badges and name badges should be returned to the Security Office at the site of employment, along with a covering note explaining why it has been sent.

7.4.3 The Security team at each site will be responsible for the destruction of returned ID badges and name badges and for updating the Swipe Card Access system and/or other relevant security databases.

7.5 Incident Reporting

7.5.1 It is essential that all security incidents are reported promptly to the Security Department at the relevant site, as follows:- LRI ext 16767; GH ext 12999; LGH ext 14292.

7.5.2 Examples of reporting timescales include:-

Instant reporting – live incidents, i.e. incident in progress, suspects still on site.

"As Soon As Possible" reporting - where liaison with Police, gathering evidence or remedial actions are required.

7.5.3 All security incidents shall also be reported using the Trust Incident Report System, Datix. It will be the responsibility of the directorate/division within which the incident has occurred, to complete the report.

7.5.4 Incidents shall be investigated and analysed in accordance with the Policy for the Reporting and Management of Incidents (including the Investigation of Serious Incidents).

7.6 Personal Property

7.6.1 **Patients** – Refer to the Trust's Management of Patient Property Policy and Procedures.

7.6.2 **Staff and Visitors** – Staff and visitors are responsible for the security of their own personal property. This includes staff and patient relatives living in the Trust's residential accommodation. These staff should make their own arrangements to have their personal property insured.

7.7 Violence and Aggression

The Trust is fully committed to protecting its staff from verbal and physical abuse. Arrangements for this are described in the Trust's Management of Violence, Aggression and Disruptive Behaviour Policy.

7.8 Nuisance or Disturbance Behaviour

7.8.1 The Trust has access to powers for dealing with low-level anti-social behaviour under Sections 119 and 120 of the Criminal Justice and Immigration Act 2008.

7.8.2 Only suitably trained staff who have attended an Authorised Officers training course can act as Authorised Officers under the Act. These nominated staff are able to authorise the removal of people under certain circumstances and will normally be called by Security staff to assist with this.

7.9 Police Assistance

7.9.1 Police assistance will normally be summoned via the Security Team or the senior manager on duty.

7.9.2 Police may be summoned, without reference to management, where delay would result in putting staff, patients or visitors at immminent risk. After such an event, the LSMS MUST be informed at the earliest opportunity.

7.10 Fraud

7.10.1 Please refer to the Trust's Counter-Fraud, Bribery and Corruption Policy A1/2010.

7.10.2 Any suspicions relating to fraud and corruption can be reported on the Confidential Fraud Hotline on 0800 0284060 or www.reportnhsfraud.nhs.uk.

7.11 Reporting Mechanisms

7.11.1 The UHL Security Management and Police Liaison Group shall be responsible for ensuring that the Trust has satisfactory policy and procedures for the security of the Trust. The Group is required to report to the Health and Safety Committee.

7.11.2 The LSMS is responsible for producing an annual report and work plan for the Audit Committee and Health and Safety Committee.

8 EDUCATION AND TRAINING REQUIREMENTS

8.1 The Trust has a duty under the Health & Safety at Work, Etc. Act to provide staff with information, instruction and training appropriate to their role. Refer to the UHL Health and Safety Policy for further detail.

8.2 Relevant staff groups will be trained commensurate with their role as defined within the UHL Core Training Policy.

8.3 The Trust provides prevention of violence training or conflict resolution training (CRT) to all its' front line staff in accordance with NHS Protect guidance and the UHL Core Training Policy. There are 3 levels of training based on risk assessment. Details of the training are provided in the Violence Aggression and Disruptive Behaviour Policy.

8.4 The training is monitored, reviewed and evaluated by the LSMS and the Conflict Management Trainer.

9 PROCESS FOR MONITORING COMPLIANCE

9.1 The Security Management and Police Liaison Group is responsible for both the monitoring and performance of the security provision across the Trust and will achieve this through the receipt of information as described in the monitoring table on Page 12, which also details timescales and the appointment of lead officers.

9.2 The results of compliance audits and security reviews/audits will be presented to the Security Management and Police Liaison Group by the LSMS and/or relevant Security Manager.

9.3 Further assurance will be provided to the Executive Team through the submission of reports by the LSMS to the Health and Safety Committee and the Audit Committee, as described in the table at the end of this policy: (page 12)

10 EQUALITY IMPACT ASSESSMENT

10.1 The Trust recognizes the diversity of the local community it serves. Our aim therefore is to provide a safe environment free from discrimination and treat all individuals fairly with dignity and appropriately according to their needs.

10.2 As part of its development, this policy and its impact on equality have been reviewed and no detriment was identified.

11 Supporting References, Evidence Base and Related Policies

11.1 This policy was developed with reference to the following documents:

- Health & Safety at Work etc, Act 1974
- The Management of Health and Safety at Work Regulations 1999
- NHS England (I) Violence Reduction standards 2020
- NHS Security Management Services no.8 – Non-physical Assaults
- "Crowded Places Guidance. Nov. 2020. Published by the National Counter Terrorism Security Office.
- "Secured by Design" (SBD) is the official police security initiative that works to improve the security of buildings and their immediate surroundings. https://www.securedbydesign.com/

11.2 The following documents are supporting policies that provide advice and guidance to managers and staff, to enable the safe management of services: This is not an exhaustive list and may be added to, as additional policies and guidance documents are created to meet identified needs:

Risk Management Policy	A12/2002
Health and Safety Policy	A17/2002
Counter Fraud and Corruption Policy	A1/2010
Management of Violence, Aggression and Disruptive Behaviour Policy	B11/2005
Major Incident Plan	available on INsite
Bomb Threat Response Plan	B1/2007
UHL Lockdown Plan	available on INsite
Closed Circuit Television (CCTV) Including BWCPolicy	B44/2005
Missing Patients Policy	B17/2005
Lone Worker Policy	B25/2008
Management of Patient Property - Policy and Procedures	B24/2007
Information Security Policy	A10/2003

12 PROCESS FOR VERSION CONTROL, DOCUMENT ARCHIVING AND REVIEW

12.1 This document will be uploaded onto SharePoint and available for access by Staff through INsite. It will be stored and archived through this system.

12.2 The UHL Security Management and Police Liaison Group through the Health and Safety Team are responsible for keeping this policy up to date.

Element to be monitored	Lead	Tool	Frequency	Reporting arrangements
LSMS work plan and overall security performance	LSMS	LSMS work plan, annual report through SMPLC Security Management police liaison committee.	4 x per annum	The UHL Audit Committee will receive the report and discuss its content with the Director Quality Governance or, in their absence, the LSMS. This discussion and subsequent actions will be formally recorded
Violence and aggression – national statistics	LSMS	NHS England– annual Reported Physical Assaults against staff (RPA)	Annually	The LSMS will complete and submit an annual RPA, as required by NHS England These figures will be published as part of Local statistics, enabling benchmarking between Trusts. The LSMS will report the national statistics to the SMPLG, the Group will identify any actions required.
Conflict Resolution Training	LSMS	Conflict Resolution Training (CRT) courses delivered and Disengagement holding skills courses Records / Statistics	Annually	Details of the number of staff trained within a financial year will be reported to SMPLG.
Police activity	LSMS	Quarterly Police site reports	Minimum four times per annum	The Police will provide reports for presentation to SMPLG members.

-End of Policy