Mid Essex Hospital Services NHS

NHS Trust

| **Security Policy** | **Corporate/Strategic**<br>**Register No:** 04051<br>**Status:** Public |
|---|---|

| | |
|---|---|
| **Developed in response to:** | Trust Requirement<br>NHSLA standards 3.9 |
| **Contributes to CQC Outcome number:** | 10 |

| **Consulted With** | **Post/Committee/Group** | **Date** |
|---|---|---|
| Helen Clarke | NHSLA Audit Lead | July 2014 |
| Jane Giles | Chief Pharmacist/ Accountable Officer | July 2014 |
| Jo Mitchell | Head of Performance, EFM | July 2014 |
| Ian Jackson | Deputy Director of EFM | July 2014 |
| Sue Brown | Head of Hotel Services | July 2014 |
| Ryan Curtis | Health and Safety Manager | July 2014 |
| Colleen Hart | HR | July 2014 |
| **Professionally Approved By** | Health & Safety Group | 19 August 2014 |

| | |
|---|---|
| Version Number | 7.5 |
| Issuing Directorate | Estates & Facilities Directorate |
| Ratified by: | DRAG |
| Ratified on: | 28 August 2014 |
| Trust Executive Board Date | September 2014 |
| Implementation Date | July 2014 |
| Next Review Date | Extension agreed to September 2019 |
| Author/Contact for Information | Eric Carter –Security/ Portering Manager; Doug Smale – LSMS |
| Policy to be followed by (target staff) | All staff |
| Distribution Method | Intranet and Website |
| Related Trust Policies (to be read in conjunction with) | Risk Management Policy and Strategy<br>Health & Safety Policy<br>Incident Policy/ Serious Incident Requiring Investigation Policy<br>Lone Worker Policy<br>Violence & Antisocial Behaviour Policy<br>Safer Restraint Policy<br>CCTV Policy<br>Controlled Drugs Policy<br>Prevention of Infant Abduction from Maternity Policy<br>Evacuation Policy<br>Mandatory Training (Training Needs Analysis)<br>Complaint handling (including the Independent Review process)<br>Supporting staff involved in a traumatic incident, complaint and claim<br>Recruitment & Selection Policy<br>Patient Missing Policy<br>Information Security Policy<br>Whistleblowing policy<br>Patient's Valuables Policy<br>PREVENT Policy |

**Document Review History**

| **Review No** | **Reviewed by** | **Issue Date** |
|---|---|---|
| 1.0 | Pepe Mengual | September 2005 |
| 2.0 | Jo Englefield | April 2008 |
| 3.0 | | |
| 4.0 | Jim Dorrian/Jo Englefield | November 2008 |
| 5.0 | Leanne Wilson | 28th October 2010 |
| 6.0 | Doug Smale – updates on job titles and roles | Dec 2012 |
| 6.1 | Jo Mitchell – update to ID application form (appendix 2) | March 2013 |
| 7.0 | Doug Smale - Formal Review | July 2014 |
| 7.1 | Jo Mitchell - Amendment to frequency of reporting to H&S Group changes to numbering, and include annual audit tool | November 2014 |
| 7.2 | Jo Mitchell - Amendment to Security Risk Assessment template | 14th May 2015 |
| 7.3 | Doug Smale - Extended for standardisation and review process | 15th January 2018 |
| 7.4 | Jo Mitchell - 6 month extension request due MSB standardisation | 6th November 2018 |
| 7.5 | 4 month extension request due MSB standardisation | 29th May 2019 |

**CONTENTS**



**APPENDICES**

## 1. Purpose

1.1 The purpose of this policy is to support the aims of the Mid Essex Hospital Services NHS Trust in the delivery of high quality clinical services through provision of a secure environment.

1.2. The standard for security management is that of supporting the Trust's strategy to provide high quality healthcare through a safe and secure environment that protects all users including patients, staff, visitors and their property and the physical assets of the Trust.

1.3. Security management in healthcare organisations is the responsibility of senior managers, but security itself is the responsibility of every member of staff and presents very real challenges in a culture where staffs are trained to put the needs of the patient first.

1.4 This policy document is intended to ensure that the Trust:

- Provide direction and help to those managers and staff who are entrusted to deal with the Trust's security provision.
- Support the delivery of high quality clinical and non-clinical services through the provision of a secure environment.
- Comply with relative legislation, such as the Health and Safety at Work Act 1974 and the Management of Health and Safety at Work Regulations 1999
- Regularly review procedures for the physical security of staff, visitors and patients as well as trust premises, equipment and information, including staffs who work in the community.

## 2. Background

2.1 The Trust is committed to providing a secure environment that protects patients, staff and visitors and their property and the physical assets of the organisation so far as is reasonably practical. This policy is part of the Trust's commitment to managing its risk agenda and acknowledges its responsibility to the wider community.

2.2 The Trust Board fully accepts its responsibility for security management matters and compliance with legislation. To this end, the responsibility will lie with the Director of Estates and Facilities Management, who will ensure that security management issues are addressed through the Health and Safety Group, which will be representative of all services.

2.3 This Policy reflects the requirements of all relevant standards and complies with relevant legislation. The Trust also fully accepts its responsibility for other persons who may be affected by its activities. The Trust will take steps to ensure that its statutory duties are met at all times.

2.4 The organisation has designated individuals as nominated officers, referred to throughout this document, whom staff / contractors may contact confidentially if they suspect a security incident has taken place. The "Nominated Officers" for the Trust are the Director of Estates and Facilities Management and the Local Security

Management Specialist (LSMS) in accordance with the Secretary of State's Directions, November 2003 and latest guidance issued from the Secretary of State for Health in November 2004 and the Security Department.

2.5 This policy does not make reference to information technology security. Please refer to the Information Security Policy.

## 3. Introduction

3.1 Whilst security management within NHS organisations is the responsibility of senior management, security itself is everyone's responsibility. Security involves all groups of staff at all levels and to be effective it is important to establish at the outset the support of everyone in the organisation. Sensible and cost effective security management initiatives can be taken to reduce risks to all stakeholders by establishing a pro-security culture, which aims to prevent criminal activity. In order to develop appropriate policies and procedures regarding security, co-operation and collaboration with other parties is essential (i.e. other organisations who may use the site, local police etc.).

3.2 It is therefore important that all those who work in the public sector are aware of, and, wherever possible, protected from the risk of illegal acts involving violence, (threatened and actual), harassment, or damage to property and theft.

3.3 The Trust Board already have procedures in place that may reduce the likelihood of breaches of security occurring. These include documented procedures and a system of risk assessment in relation to the physical security of Trust premises and assets in accordance with NHS Protect. In addition, the Board aims to ensure that a risk aware culture exists within the Trust and has complied with the Secretary of State's Directions in nominating a Local Security Management Specialist (LSMS).

## 4. Aims

4.1 The policy seeks to ensure:

- The personal safety at all times of all the Trust users
- The protection of property against fraud, theft and damage, or the potential threat of terrorist activity
- A safe environment in which the uninterrupted delivery of quality health care can be delivered
- A partnership with local agencies, e.g. police and local authority for a safe and secure Trust environment
- staff are provided with appropriate information and/or training on security initiatives and best practice

## 5. Scope

5.1 This policy applies to all staff, visitors and patients attending or working for the Trust, including contractors and staff working in the community.

## 6. Roles and Responsibilities

The Trust has appointed a number of key employees to have managerial and supervisory responsibilities for ensuring compliance to this policy, legislation and liaison with external stakeholders (e.g. police, NHS Protect).

### 6.1 Chief Executive

The Chief Executive has overall responsibility for controlling and co-ordinating security. However, responsibility for management and implementation of this policy is delegated to the Security Management Director (SMD) and the appointed LSMS. This is in accordance with the Secretary of State Directions of November 2004 and the Security Incident Response plan.

### 6.2 Security Management Director (SMD)

The SMD (Director of Estates and Facilities Management) will be responsible for taking reports and proposed action plans to the Chief Executive and the Executive Team for consideration and implementation. The SMD may delegate various responsibilities to an appropriate manager and/or the appointed LSMS and is required to monitor and ensure compliance with directions set out by the Secretary of State on NHS Security Management. The SMD will report any amendments of this policy to the Trust Board.

### 6.3 Local Security Management Specialist (LSMS)

6.3.1 The LSMS provides a resource to managers at all levels in the pursuit of incident investigations. This will also involve carrying out surveys, audits and risk assessments for and with departments to promote safer working arrangements and environments.

The LSMS must:

- have been approved by the NHS Protect as a suitable person for appointment
- have successfully completed any training required by NHS Protect
- report directly to the Designated SMD on all security issues
- not undertake responsibility for the counter-fraud activities of any NHS body

6.3.2 The LSMS will provide all the necessary advice to ensure that the policy is in operation within the Trust.

6.3.3 The LSMS is responsible for the Implementation of a Crime Reduction Plan, Incident Response Plan in conjunction with the Security and Portering Manager.

6.3.4 The LSMS is responsible for monitoring security risk assessments in conjunction with the Security and Portering Manager.

6.3.5 The LSMS is responsible for co-ordinating investigations and incident follow up, including providing support and clarification to victims of crime regarding process. The LSMS is also responsible for promoting and developing a pro-security culture within the Trust by raising the profile of incident reporting and redress in accordance with the procedures set by NHS Protect.

6.3.6 The LSMS has a duty to provide support and guidance to victims as necessary and assist the police in pursuance of any investigations that follow. The LSMS will attend court appearances with staff when required, and provide a presence during all cases representing the Trust.

6.3.7 The LSMS will lead on the Hospital Watch Scheme Initiative for the Trust and work in conjunction with the North Essex Mental Health Partnership Foundation Trust and Essex Police to ensure joint working across healthcare sites relating to crime reduction.

6.3.8 The LSMS is responsible for liaison with persons responsible for security at other local NHS organisations, East of England Ambulance Trust, Essex Air Ambulance, Essex County Council and local Borough Councils and the Police.

### 6.4 Governance Department

6.4.1 The Governance department are responsible for ensuring that procedures are in place to allow the Trust to actively pursue incidents and that a successful reporting culture is developed and enforced

6.4.1 To incorporate security into the Trust Risk Management strategy, by collating and monitoring security incidents and risks highlighted in conjunction with all incident reports to identify trends or perceived risks.

6.4.2 Reports of serious incidents relating to major theft, loss, and any form of violence, non-violence and harassment are to be forwarded to the LSMS to monitor and make NHS protect aware.

### 6.5 Portering &Security Manager

6.5.1 The Portering & Security Manager is responsible for ensuring:

- the effective running and delivery of a security service within the Trust
- any contracted security company provides adequate security staff who are vetted and licensed according to the SIA (Security Industry Authority)
- security staff are adequately trained, in particular in Conflict Resolution, and provided with the appropriate Personal Protective Equipment (PPE) to allow them to carry out their roles in confidence and as safe as possible
- security Officers respond to incidents in the appropriate manner and ensuring that all such incidents are reported via the Trust Datix incident reporting system
- the effectiveness of the CCTV, intruder alarms, access controls, lighting and key related access processes through monitoring (in conjunction with the LSMS)
- they work with the LSMS relating to all security issues to ensure that the Trust and NHS Protect security strategies are implemented

## 6.6 Security Officers

6.6.1 Security Officers should be informed of any events and issues; they in turn will notify and report findings to the Portering & Security Manager or LSMS as appropriate. Reports in the form of Risk Event forms (Datix) will also be referred to the LSMS.

6.6.2 Security Officers are responsible for assessing security risk and for immediate action and notification of incidents. Where possible, in the first instance, they are to attempt to dispel and control incidents sufficiently that the risk is reduced and care can continue. In addition, they are the initial liaison for the police etc. should they be requested to attend: following their liaison with the police they must notify the LSMS by an appropriate means i.e. telephone, email etc.

## 6.7 Accountable Officer (AO) Controlled Drugs (CDs)

6.7.1 The Chief Pharmacist is the Accountable Officer (AO) for the Trust. The AO is ultimately responsible for all aspects of the safe and effective use of CDs within the Trust. Any staff concerns about individuals or processes in the handling of CDs should be reported to the AO. See also the Controlled Drugs Policy.

## 6.8 All Directors, Heads of Nursing, Lead Nurses, Managers and Supervisor Staff

6.8.1 It is the responsibility of directors and managers to ensure that they and their staff fully comply with the security policy, and follow the incident reporting policy and system when a breach of security occurs.

6.8.2 Security is a responsibility of managers who must undertake preventative measures for the safety of staff, users and property.

6.8.3 Managers should implement a procedure to record details, of any valuable property left in their care, ensuring that arrangements are made to secure the department out of working hours, together with the safe custody of keys.

6.8.4 Managers should keep records of all keys issued to staff and report the loss of keys to the Portering & Security Manager.

6.8.5 Managers should advise the security department of any changes within departments that may adversely affect the overall security of the premises. Managers should also update their security risk assessment at this time and forward to the LSMS.

6.8.6 Managers should ensure all staff employed by the Trust, or from other organisations working in the Trust, including contractors and visitors, will wear an identification badge/ card at all times.

6.8.7 Managers must ensure that all members of staff are made aware of the above policy and fully understand its content and their responsibility under the policy and that they are required to communicate this to their staff.

6.8.8 To enable effective security management, senior managers must monitor and report on the workplace to ensure that the Trust is protected. Where security management risks are identified the manager must ensure that these are assessed, eliminated or minimised, so far as is reasonably practicable.

6.8.9 Contracted staff are expected to adhere to the Trust Security Policy and Trust staff letting and managing contracts/contractors are responsible for ensuring security is maintained.

6.9 **Human Resources (HR)**

6.9.1 HR will ensure all pre-employment screening is undertaken and a robust vetting procedure is adopted in accordance with NACTSO (The National Counter Terrorism Security Office) and NHS Protect Requirements.

6.10 **All Staff**

6.10.1 All staff has a responsibility to report any breaches or incidents of a security nature. The main forum for this will be via the Trust's Incident reporting system (Datix). Where urgency dictates, incidents can be reported via Security Operatives, and / or the LSMS.

6.10.2 All staff of the Trust has a duty to be aware of the Security Policy and to adhere to it. Staff must co-operate with management to achieve the aims, objectives and principles of the security policy. Great emphasis is placed on the importance of co-operation from staff in observing security measures and combating crime at all levels. Security concerns, incidents including incidents of violence and aggression should be reported immediately to line managers and an incident report should be completed as soon as possible.

6.10.3 Staff should be aware of their responsibilities in protecting at all times the assets and property of patients, visitors, colleagues and other Trust users, as well as the safety of the Trust's assets and property.

6.10.4 Where specific security procedures exist, staff must abide by them at all times. Where staff know or suspect a breach in security, they must report it immediately to their manager and escalate it to the LSMS/ Security Officers. Once escalated, a Datix report form must be completed detailing the breach.

6.10.5 All staff are reminded that it is an offence to remove property belonging to the Trust without written authority. Failure to seek authority from their line manager could result in disciplinary action or criminal prosecution.

6.10.6 Staff are required to wear an identification badge whilst on duty for the Trust, this also applies to those that are at work in the Community.

6.10.7 Staff are responsible at all times, for the protection and safe keeping of their own property. The Trust LSMS will if requested, advice staff on the security of their property, including motor vehicles or other modes of transport. Any theft of private property must be reported to police without delay. If property has been brought on site, it is at the owner's own risk and therefore it is their responsibility to report the incident.

## 7. How Security fits in with Other Organisational Functions

7.1 The overlapping interests of security with the requirements of the Health and Safety legislation and the preventive and protective elements of fire and safety are recognised. The LSMS will maintain close liaison with the Security and Portering

Manager, Trust Fire Officer, the health and Safety Manager and all managers and supervisors to ensure that in implementing security any threat to life, property and the means of escape are fully considered in conjunction with Fire Policy and guidelines. In addition all these functions will be subject to internal audit.

7.2 Advice on security matters should initially be sought from an immediate supervisor or manager who may refer to the LSMS who will have recourse to relevant security manuals. The NHS publishes information on security/personal safety, which will be held and distributed as appropriate by the LSMS. Reference should be made to the Fraud/Whistle Blowing and Violence and Aggression Policies where appropriate.

7.3 It is acknowledged that all members of staff have a right, as individuals, to refer to the police if they feel threatened in any way in the course of carrying out their duty. Without seeking to prejudice that right, the automatic involvement of the police may not always be in the interests of involved parties, the Trust or the police themselves. Therefore it is suggested that in **non-emergency** situations, staff should consult with the LSMS or their line managers in the first instance. Similarly, it is recommended that, where practical, line managers discuss incidents with the LSMS prior to a referral to the police.

## 8. Building and Refurbishment Projects

8.1 The Trust will ensure suitable advice regarding security is sought and that appropriate security measures are incorporated into all buildings projects and developments.

8.2 All capital and revenue projects involving changes to, or the introduction of, security devices must be referred to the LSMS who will in turn seek assistance and consultation with the Police Crime Prevention Design Advisor. The LSMS will also advise the Trust on relevant Health Technical Memorandum's (HTMs) or other papers released.

## 9. Reporting and Controls

### 9.1 Incidents

9.1.1 All security incidents should be reported by telephone on 6000 or bleep to the Security lead, Team Leader (on shift). **For emergency contact fast bleep 6666 is the recommended method.**

9.1.2 Incidents should be recorded, by the reporting department, on the Trust's electronic Incident Report form (DATIX). The Manager for the area will be required to investigate the incident and the Security Porters manager and LSMS should be alerted.

9.1.3 Security Officers will complete a security incidents form when requested to attend security incident. This log will be maintained by the Portering and Security Department. Security Officers are responsible for completing Trust's Incident Report form when an incident has occurred in a public area.

9.1.4 Incidents involving theft of or damage to Trust property should, in addition, be reported by telephone to Departmental Management, Portering & Security Manager and LSMS.

9.1.5 Serious Security Incidents should be reported to the Portering & Security Manager and LSMS.

9.1.6 Incidents of violence and anti-social behaviour will be managed by the SMD, who will delegate as appropriate to the LSMS.

9.1.7 A log is kept of reported security incidents. This is maintained by the Hotel Services Department.

## 9.2 Security Incident Data Analysis

9.2.1 Individual incidents will be reviewed by the LSMS upon receipt to ensure that they have been completed in accordance with this policy and CFSMS guidelines

9.2.2 Incident figures will be collated through the Trust's incident reporting procedures. Relevant incidents will be sent to NHS Protect on a regular basis in accordance with their national monitoring system SIRS (Security Incident Reporting Service) by the LSMS.

9.2.3 The Health and Safety Group will review summaries of security incidents and trends analysis on a consistent basis. Where this review identifies areas at a high risk of incidents, further support, including advice and additional training will be provided by the LSMS**.**

9.2.4 Significant risks will be recorded and placed on the Risk Assurance Framework with appropriate controls and risk treatment plans in operation within the directorate, who will ensure adequate business planning to reduce or remove the risk, so far is reasonably practicable.

## 9.3 NHS Protect Alerts

9.3.1 Alerts are issued on Security and individuals who may pose a significant threat to NHS staff or patients. These Alerts are issued by NHS Protect and detail recommendations to be implemented by the organisation to protect its staff. If an alert is received by a department the Department Manager must ensure all listed recommendations are actioned and report back to the LSMS.

## 9.4 Health and Safety Group

9.4.1 The Trust has an established Health and Safety Group with representatives from all areas of the Trust. The Group has agreed terms of reference and will:

- Receive information and reports from the LSMS in the form of a security report on incidents and all security matters at each meeting and a report to be presented annually.

- Conduct post incident reviews and, in consultation with the LSMS, co-ordinate a Trust wide action plan to address any shortfalls and to implement appropriate recommendations in accordance with NHSLA guidance.

- Jointly identify any anticipated need for action or, where applicable, escalate issues for discussion at Board level through the chair of the Health and Safety Group/ SMD.

- Review current policy and processes with a view to upgrade or improve security measures and hardware.

## 9.5 Requirement to undertake appropriate risk assessments.

### 9.5.1 Proactive assessment

- Annually, managers should undertake appropriate security risk assessments for their areas of responsibility using the Trust Security Risk Assessment template (see Appendix 1) in respect of the prevention and management of security incidents.

- These proactive risk assessments should be reviewed annually as a minimum and more frequently if necessary in order to address any foreseeable weaknesses, such as the introduction of new buildings, new services or a significant change in use of an area.

- Where the Trust is in receipt of intelligence which might result in an incident associated with security, a risk assessment should be undertaken to evaluate and address any risks identified.

- Where risks are identified, an action plan should be developed with clear timescales and any significant risk should be recorded on the Directorate and Health and Safety Risk Assurance Frameworks. Progress should be monitored locally by departmental leads.

### 9.5.2 Reactive assessment

- Reactive risk assessments are carried out post event using the template in Appendix 1. Generally these may be after an incident has occurred or as a result of an identified weakness in current practice.

- Where risks are identified, an action plan should be developed with clear timescales and this risk should be recorded on the Directorate and Health and Safety Risk Assurance Frameworks and an action plan developed

### 9.5.3 Escalation of Security Risks and Risk Assurance Framework (RAF)

- All services will review their risks with respect to security management using the security risk assessment tool (see Appendix 1).

- All identified security management high risks (rated 15 and above) must be entered onto the appropriate directorate RAF and the Health and Safety RAF.

- Significant risks must be managed in accordance with the Risk Management Strategy.

9.6 **Risk Book**

9.6.1 The Risk Book is a folder situated in all clinical departments containing information relating to health, safety, security and welfare of staff.

9.6.2 Staff are responsible for ensuring their risk assessment for security are kept up to date and information and intelligence about new risks are shared with staff working in the department, the Portering and Security management and the LSMS.

9.6.3 Risk assessments in the risk books will also be stored electronically in a shared data location for monitoring purposes within the Governance department.

## 9. Specific Areas of Security

10.1 **Security of Equipment**

- All portable equipment should be kept in a secure place, particularly at times when departments are not staffed. Managers are to maintain an inventory/asset register of equipment within their department that is in excess of a value of £1,000. However, this figure may vary as directed by the Director of Finance.

- The register must be verified on an annual basis and adjusted when new equipment is obtained. All equipment must be clearly marked with the name of the hospital/departmental/ward as soon as it is obtained and any loan of equipment to other departments/wards should also be entered in the register, albeit temporarily

10.2 **Security of Employee's Property**

10.2.1 Employees are advised not to bring large amounts of money, valuables to work or any item that might present a security threat/ risk to work.

10.2.2 Where changing facilities are provided for employees, the room should be kept locked to prevent unauthorised access. Lockers, when available, should be used for all personal property. In the event of deficiencies or un-serviceability, the Estates & Facilities Help Desk should be informed via the line manager.

10.2.3 All instances of theft of property should be reported immediately to the manager and on an Incident Report form (Datix).

10.2.4 All staff are to be made aware that all money and valuables are brought onto Trust premises at the owner's own risk. Staff have a duty to take reasonable steps to ensure the security of their personal belongings whilst at work, and take consideration of personal items that they bring into the work environment

10.3 **Asset Marking**

10.3.1 The Head of Department should keep an inventory of all equipment within their charge and regular checks should be made to ensure the equipment is where it should be.

10.3.2 It is the responsibility of Departmental Managers to ensure that equipment and the inventory are logged onto an asset register and stored within the department for audit and monitoring purposes.

## 10.4 Patient's Property

10.4.1 Patients' property should be handled in accordance with Trust policy for managing patient's valuables policy and secured accordingly.

10.4.2 No responsibility can be accepted by the Trust for the loss of personal property that is not stored as per 10.4.1.

10.4.3 Suitable and sufficient documentation should be completed to record personal items of patients while on Trust premise. In addition, guidance should be given to patients by the Trust and individual departments on the suitability of bringing valuable items onto Trust premises. However, it is the responsibility of the patients, visitors and contractors to make sure that their personal property is secure.

## 10.5 Lost Property

10.5.1 All found property should be immediately handed to the Duty Security/ Porters Supervisor. Compliance to the Trusts' Standing Financial Instructions for lost property shall be implemented

## 10.6 Trust's Right to Search Property

10.6.1 Legally the Trust is entitled to authorise trained security operatives with powers to search lockers property etc. following declaration of an incident where an item (of any description) is reported missing.

10.6.2 Security Officers have the right to ask for staff to empty pockets, bags, lockers etc. to rule out any alleged offence on Trust premises.

10.6.3 Security Officers do not have the right to frisk, touch or physically search a person. This function is the sole responsibility of the Police. Should security operatives suspect a person is concealing an item on their person, the police will be informed and requested to attend for a search.

10.6.4 Security Operatives are not to compromise any situation where a crime scene scenario may apply: crime scene integrity must be retained for the police. If at any time the Security Operatives suspect a crime has taken place, the Operatives must notify the LSMS and Security/ Porters Manager to secure the crime scene and preserve evidence.

10.6.5 Trust employees have the right to refuse a search of their property or to empty pockets etc., but in doing so this will lead to HR and police contact to conduct a search. The purpose of the search is for the protection of staff to minimise the risk of allegations made by patients, members of the public and other staff.

## 10.7 Access Control and Trust Identification Badges (Appendix 2)

10.7.1 Photographic identification should be worn at all times Trust-wide and the security policy supports the policy of all staff wearing up to date photographic identification

badges. A computerised photo ID badge scheme combined with access control proximity card operates in the Trust. Staff responding to a major incident must bring photographic ID with them, as this will be needed to access the hospital as access may be restricted by the police.

10.7.2 Staff who are not wearing an identification badge should be challenged and requested to wear their badge. Failure to visibly wear a personal ID badge is a disciplinary matter.

10.7.3 The Departmental Manager and Portering Security Manager are able to determine levels of security access to buildings and internal areas throughout the Trust.

10.7.4 Identification badges are the property of the Trust and under no circumstances should they be worn by, or transferred to, any other person than the holder. Staff are not to allow any other individual to use their access card/fob at any time and should not allow any other person passage through any access point. All staff entering a restricted area are required to present their card prior to entry.

10.7.5 Staff are not to leave controlled doors open or unattended at any time. Visitors needing access to restricted areas should be escorted at all times.

10.7.6 Persons not wearing an identification badge and those whose identity is unknown must be challenged and asked to account for their presence. This should be done politely and quietly and in a helpful manner. Suspicious incidents must be reported to Security as soon as possible and an Incident Report completed.

10.7.7 Lost or stolen identification badges and all problems relating to the proximity card system (including lost, missing or stolen cards) must be reported to your Line Manager and Security Porters immediately.

10.7.8 When a staff member leaves the employment of the Trust, it will be the responsibility of the departmental manager to retrieve the identification badge and arrange for the deactivation and destruction of the card

10.7.9 The operational management and control of this system kept within Estates and Facilities. The protocol for effective management is followed. In addition, alterations to the permissions of access may be altered dependent on need.

### 10.8 **Closed Circuit Television (CCTV)**

10.8.1 The Trust will comply with legislation such as the Data Protection Act and other related legislation that ensures full compliance with the law. This will be controlled by the Estates and Facilities directorate to ensure that propriety and professional use is maintained.

10.8.2 In addition the LSMS and Portering and Security Manager will assist and ensure that the Trust's protocol for controlled use of the CCTV systems throughout the Trust premises is followed in accordance with the Trusts' CCTV policy.

### 10.9 **Security Alarm Systems**

10.9.1 It is the responsibility of Heads of Department or a designated member of staff to activate their local alarm system on leaving the building or deactivate the alarm on re-

entering the building. Switchboard will notify the Security operative should an alarm be activated within a designated building.

10.9.2 Personal and Departmental panic button alarms systems are employed in a number of areas throughout the Trust presently. Each of these is considered through a risk assessment process.

10.10 **Lockdown**

10.10.1 Lockdown is the process of controlling the movement and access, both entry and exit, of people (NHS Staff, patients, visitors and public) around Trust sites or other specific trust buildings or areas in response to an identified risk, threat or hazard that might impact upon the security of those on site or the capacity of the organisation to continue to operate. A lock down is achieved through a combination of physical security measures and the deployment of security personnel.

10.10.2 The Portering and Security Manager will co-ordinate an electronic system to establish up-to-date site, buildings and security profiles in line with NHS Protect Lockdown Guidance for each Trust site. The Fire and Security Advisor will identify gaps in information and liaise with Estates and emergency planning functions.

10.10.3 All managers for each department must ensure they have addressed lockdown in their department security risk assessments and ensured that all staffs are aware of the local lock down procedure for the area.

10.11 **Security of Motor Vehicles**

10.11.1 All motor vehicles used by employees, patients, and visitors along with other outside agencies must park in the authorised parking areas which have been provided by the Trust.

10.10.2 The security of motor vehicles owned by employees, patients and visitors is the responsibility of the owner of the vehicle. Whilst the Trust provides parking facilities, it does not accept liability for any theft, loss or damage to motor vehicles or their contents when they are parked on the Trust sites. See also the Trust's Car Parking Policy.

10.11 **Security of all Residences**

10.11.1 Staff whom are residing in the Hospital accommodation should be advised that they are responsible for their personal property and should insure it against theft/damage. Wherever possible it should be locked away out of sight during the absence of the owner.

10.11.2 The Trust is not responsible for the security of hospital accommodation this is the responsibility of the housing association.

10.12 **Keys and security access devices**

10.12.1 Keys and security access devices are important security items and must be kept on the person at all times. Under no circumstances should these be left unattended e.g. on desks, in key holes of doors, or borrowed by unauthorised personnel.

10.12.2 Managers have a responsibility to ensure that their department is locked when unoccupied and for ensuring that only named members of staff have keys to that site.

10.12.3 Duplicate keys and security access devices should be held in a locked cupboard/cabinet.

10.12.3 Arrangements must be made to ensure that adequate arrangements are in place for opening and closing of departments, which are cleaned by domestic staff outside normal working hours.

10.12.4 Replacement keys are only to be obtained via the Estates department and must not be replicated locally. Reimbursement for replacement keys will not be made via Petty Cash: the cost of replacement is to be met by the requesting services.

10.12.5 The issue of Master suited key systems and keys and devices should be severely limited and only issued to those staff responsible for whole areas of a building.

10.12.6 Staff who hold access devices must also be made aware that losing them could be a high security risk and they are accountable for them.

10.12.7 If access devices are lost, staff may be charged for their replacement, dependent upon the circumstances of the loss.

10.13 **Security of Controlled Drugs (CDs) and CD Cupboard Keys**

10.13.1 If the CD keys cannot be found then urgent efforts should be made to retrieve the keys as speedily as possible by contacting nursing staff who have just gone off duty, or others who may have been given access to the keys e.g. Authorised Pharmacy Staff. The Chief Pharmacist, Chief Nurse or senior Nurse on duty should be informed as soon as possible.

10.13.2 If the keys are not located within 24 hours the Accountable Officer will be informed by the relevant staff mentioned above. Depending on the circumstances it may be appropriate to contact the police; this decision will be made by the Accountable Officer. If wrong doing is suspected, the police should be involved.

10.13.3 For further details on the management of security requirements of Controlled Drugs please refer to the Controlled Drugs Policy.

10.14 **Intruders/ Unauthorised/ Suspicious Persons**

10.14.1 The Trust has an undertaking to provide suitably qualified security staff who can be called in an emergency.

10.14.2 If an unauthorised person/s is found on the premises, Security Officers have the authority to ask them to leave, escort them from the premises using reasonable force, as dictated by the Security Industry Authority (SIA) Guidelines, or to notify the police, depending on the situation presented at the time.

10.15 **PREVENT**

10.15.1 Should any member of staff have concerns relating to an individual's behaviour which indicates that they may be being drawn into terrorist-related activity, they will need to take into consideration how reliable or significant the indicators are. All staff

must raise their concerns and seek advice on how to address them in accordance with the Trusts PREVENT Policy.

10.15.2 Staff can seek advice through the Trust's PREVENT Operational Lead, alternatively advice is also available through the Trust's Safeguarding Team, and out of hours advice can be sought via the Trust's Clinical Site Managers / On-call Senior Manager.

10.15.3 Where staff believe that concerns may need to be escalated, they should seek advice from the Trust's PREVENT Operational Lead / Safeguarding Team, who will assist in determining whether the matter needs to be referred on.

**11. Data Protection** – Staff should refer to the list of information governance and information security policies listed in their Information Governance Handbook that is issued to all staff.

## 12. Training

12.1 HR and the Learning and Development departments are responsible for ensuring that security awareness is included in Corporate Induction training and that all front line staff in high risk areas receive mandatory conflict resolution training in accordance with NHS Protect guidance.

12.2 All security staff will be required to be trained in managing violence and aggression and breakaway training on an annual basis.

12.3 Any further training will be delivered in accordance with the Trust's Training Needs Analysis which will include staff groups at high risk such as A&E staff.

## 13. Communication and Implementation

13.1 The policy will be made available on the Trust's intranet & website.

13.2 The approved policy will be notified to all staff via the Trust's Staff Focus.

## 14. Monitoring and Compliance with Policy

14.1 Policy effectiveness will be monitored by Health and Safety Group through feedback from security representatives.

14.2 NHS Protect compliance will be submitted NHS Protection the form of an Annual Report and Security Work plan annually.

14.3 A further measure of compliance will be continual communication with external stakeholders by the LSMS to ensure that all available endeavours are met.

14.4 An annual audit of compliance with this policy will be undertaken in a representative sample of areas by the LSMS and the Portering and Security Manager (see Appendix 3). As a minimum this will assess the following:

- whether appropriate security risk assessments to assess the physical security of premises and assets have been undertaken;
- whether actions were developed and implemented where indicated

- whether identified security weaknesses were reported to the Health & Safety Group
- Whether the Security Annual report and Work plan were submitted.

14.5 The results of the audit will be reported to the Health and Safety Group and an action plan to address any identified deficiencies will be developed with implementation monitored by the group at subsequent meetings.

## 15. Review

**15.1** This policy will be reviewed in 3 years or earlier as a result of staff change, local or national initiatives.

## 16. References

- The Health and Safety at Work Act (etc.) 1974 (2) and (3)
- Management of Health and Safety at Work Regulations 1999
- Reporting of Injuries Diseases and Dangerous Occurrence Regulations 1995
- NHS Security strategy “A professional approach to managing security in the NHS 2003
- Directions to NHS Bodies on measures to deal with violence against NHS staff 2003 amendments) Direction 2006
- Directions to NHS Bodies on Security Management Measures 2004
- Prevention and Management of Violence where withdrawal of treatment is not an option 2003
- Not Alone- guidance for the better protection of lone workers in the NHS 2003
- Procedures for placing a risk of violence marker on electronic and paper records 2010.

**Appendices**

| | | |
|---|---|---|
| Appendix 1 | Security Risk Assessment Template | Security Risk Assessment Template |
| Appendix 2 | Application for ID Badges | Security ID Form Aug 2014.doc |
| Appendix 3 | Annual Security Policy Audit Tool | Appx 3 - Security Policy Audit Template |