SECURITY MANAGEMENT POLICY
(Including Physical Security of Premises and Assets)

<table>
<thead>
<tr>
<th>Version:</th>
<th>V4.4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Author:</td>
<td>Darrell Linton</td>
</tr>
<tr>
<td>Designation:</td>
<td>Local Security Management Specialist</td>
</tr>
<tr>
<td>Responsible Director:</td>
<td>Director of Nursing &amp; Quality</td>
</tr>
<tr>
<td>EIA Assessed:</td>
<td>12 February 2013</td>
</tr>
<tr>
<td>Target Audience:</td>
<td>All Trust Staff</td>
</tr>
<tr>
<td>Approved By:</td>
<td>Policy Review Group</td>
</tr>
<tr>
<td>Approval Date:</td>
<td></td>
</tr>
<tr>
<td>Ratified By:</td>
<td>Policy Review Group</td>
</tr>
<tr>
<td>Ratification Date:</td>
<td></td>
</tr>
<tr>
<td>Review Date:</td>
<td>February 2016</td>
</tr>
</tbody>
</table>

If printed, copied or otherwise transferred from the Intranet, Trust-wide Corporate Business Records will be considered 'uncontrolled copies'. Staff must always consult the most up to PDF version which is on the Intranet.
# CONTENTS

1. Introduction ........................................................................................................ 3  
2. Purpose .............................................................................................................. 4  
3. Definitions .......................................................................................................... 4  
4. Duties/Responsibilities ..................................................................................... 5  
5. Process ............................................................................................................ 10  
6. Consultation ..................................................................................................... 21  
7. Implementation ................................................................................................ 21  
8. Training and Support ...................................................................................... 21  
9. Review .............................................................................................................. 22  
10. Monitoring Compliance .................................................................................. 22  
11. References ....................................................................................................... 22  
12. Trust Associated Documents .......................................................................... 23  
13. Version Control ............................................................................................... 23  

Appendix 1 .............................................................................................................. 26  
Appendix 2 .............................................................................................................. 27  
Appendix 3 .............................................................................................................. 29
1. Introduction

This policy is designed to ensure that the delivery of healthcare takes place in a safe and secure environment, free from the risks of crime which may arise when providing a public service, in line with the requirements of NHS Protect.

Coventry and Warwickshire Partnership NHS Trust are committed to meeting the requirements of the NHS Protect’s anti-crime strategy as laid out in the document ‘Tackling crime against the NHS – A strategic Approach’ and the document ‘Standards for Providers – Security’ (see Appendix 2 for more information).

Local arrangements for the delivery of the aims of the NHS Protect Strategy include the nomination of an Executive Director as the Security Management Director (SMD), Non-Executive Director (NED) to support the development of security management at the Trust, and the provision of the services of a Local Security Management Specialist (LSMS) to advise on the day-to-day security issues at the Trust.

Coventry & Warwickshire Partnership NHS Trust provides the following services Mental Health, Learning Disabilities and Community Services.

The organisations interacts with NHS Protect via Regional LSMS quarterly meetings, sector meetings (Mental Health & Learning Disabilities) and when seeking advice from the Area Security Management Specialist on NHS Protect policies, protocols, guidance, best practice and on local issues, such as warning letters.

During November 2011 the protocol ‘Tackling Violence and Antisocial Behaviour’ joint working agreement between the Association of Chief Police Officer, the Crown Prosecution and NHS Protect (NHS Business Services Authority website) replaced the existing memorandums of understanding between the above organisations. This protocol will be implemented locally by a service level agreement between the parties and any other organisations or bodies that the parties think appropriate.

This Policy applies to all staff employed by the Trust, either directly or as part of a contracted service, and to any other person or organisation that uses Trust services or premises for any purpose. All staff has a core responsibility to ensure that local security measures and procedures are observed at all times. Specific roles and responsibilities of nominated staff with regards to security management are detailed in Section 3 of this Policy document.

The Policy directions shall be adopted Trust wide but it should be recognised that local procedures and protocols should continue to be developed and implemented to support the Policy.
2. **Purpose**

The purpose of this policy is to advise and support Trust staff on security matters and to seek their support and commitment to ensure that all staff undertakes an active role to ensure a safe and secure working environment is maintained and pro-security culture is created.

Further information contained in this document shall outline the structure required, specific directions, guidance on security management and operational issues, including the roles and responsibilities of nominated persons to ensure that the policy is effectively implemented.

The main aim of this policy is to integrate the management of security into existing practice and governance arrangements adopted by the Trust to ensure the following:

- The personal safety and well being, at all times, of patients, staff and visitors, is not unduly compromised.
- Adequate protection is afforded to protect the Trust’s assets and buildings from theft, malicious acts and criminal damage.
- All reported breaches of security are identified and investigated in a fair and objective manner.

Section 5 outlines some examples of the processes in place which contribute to the Management of Security within Coventry & Warwickshire Partnership NHS Trust.

3. **Definitions**

3.1 **Physical Assault**

The intentional application of force against the person of another without lawful justification, resulting in physical injury or personal discomfort.

3.2 **Non-physical Assault**

Non-physical assault – the use of inappropriate words or behaviour causing distress and/or constituting harassment.

3.3 **Lockdown**

A lockdown is the process of preventing freedom of entry to, exit from or movement within the Trust.
4. Duties/Responsibilities

4.1 Chief Executive

The Chief Executive has overall responsibility and accountability for the implementation of all aspects of this policy and to ensure that the organisational commitment to security management is fully met and monitored. The Board recognises that a successful healthcare organisation ensures that its expertise in service provision is translated into all aspects of its work and that effective security management is an integral part of effective work practice.

Operational responsibility is delegated to the Director of Nursing & Quality.

4.2 Director of Nursing and Quality

The Trust’s Director of Nursing & Quality undertakes the role of Security Management Director and shall take overall responsibility for overseeing security management work and ensuring compliance with Secretary of State directions and subsequent guidance issued by NHS Protect, as well as ensuring that the Local Security Management Specialist (LSMS) has the necessary resources and support available to carry out their role effectively.

Reporting directly to the board the SMD will be responsible for ensuring that there are appropriate up to date security management services and specialist advice available within the Trust. The SMD will also be responsible for ensuring that effective systems and work practices are in place and for promoting preventative security measures throughout the Trust.

4.3 Nominated Executive Director (NED)

The principle role of the NED, as set out in Secretary of State Directions, is to promote the security issues and needs of the health body, to support and, where appropriate, challenge the SMD with regard to their security management responsibilities at board level. The NED’s purpose is to promote security management measures by making certain that the SMD is undertaking the role effectively and in accordance with legal requirements and NHS Protect guidance. This role is carried out by a non-executive Director.

4.4 Health, Safety & Security Committee

The Health, Safety and Security Committee is accountable to the Operational Safety & Quality Committee.
The Committee will:

- Provide assurance on health, safety and security performance to the Trust Board via the Operational Safety and Quality Committee.
- Undertake and report back on the Committee's Annual Programme of Work.
- Establish and review a performance/assurance Framework, for health, safety and security within the Trust.
- Ensure that the Trust receives adequate specialist advice in all areas of health, safety and security.
- Identify key risks, review and monitor associated incident statistics and trends, and make recommendations for action as appropriate.
- Receive and consider health, safety and security reports, including incident investigations, from specialist advisers, external inspectors and staff representatives and make recommendations as appropriate.
- Monitor and analyse associated performance data (e.g. inspections, training, etc).
- Develop and approve health, safety and security strategies and associated policies.
- Act as the central point for consultation on new and revised policies relating to Health, safety and security.
- Oversee the implementation of health, safety and security policies and be responsible for their review.
- Receive and synthesize pertinent national reports / evidence and make recommendations for local practice as required.
- Promote health, safety and security across the Trust.
- Develop annual work plans for health, safety and security.
- Produce annual report for health, safety and security.

The Health, Safety and Security Committee will report to the Operational Safety and Quality Committee.

A summary report will be provided to the Safety & Quality Operational Committee on a bi-monthly basis (following each meeting).

4.5 Violence and Personal Safety Committee

The Violence and Personal Safety Committee (VPS) is accountable to the Operational Safety & Quality Committee.

The Committee will:

- Ensure that appropriate frameworks are in place to identify and act on issues relating to violence and personal safety within the various service delivery areas.
- Identify and recommend any changes and/or development of practice, training, policies and standards, necessary to support the
safe delivery of services by the Trust with specific regard to mitigating against violence and ensuring individuals personal safety.

- To receive and address SIRI and incidents resulting in staff absence and RIDDOR reportable incident reports and associated action plans pertaining to the role and function of the committee including verbal and physical aggression, restraint and relevant security incidents.

- To develop an overview of incidents of violence, aggression and personal safety from across the Trust with the aim of early identification of themes and/or trends enabling early intervention.

The VPS is a sub committee of the Trust Safety and Quality Committee and will provide regular reports via the Safety and Quality Operational Committee.

The Committee Structure is attached as Appendix 1.

4.6 Local Security Management Specialist (LSMS)

The role of the LSMS is primarily to deliver security management work locally to agreed national standards as set in Secretary of State Directions. The post holder will be responsible for the following:

- Ensuring that appropriate steps are taken to create a pro-security culture.
- Arrange for security awareness to be included as part of the staff induction process.
- Undertaking crime reduction work including crime reduction surveys.
- Develop and review local and organisational action plans to implement solutions to security risks identified during risk assessments.
- Implement and maintain active and reactive monitoring to ensure adherence to security policies and physical security requirements.
- Undertaking investigations of security breaches and reporting as required by NHS Protect guidance.
- Ensuring that where a member of staff has been assaulted that appropriate support/counselling has been made available.
- Ensuring that lessons learned are fed into further risk analysis and crime reduction work.
- Working with the SMD and NHS Legal Protection Unit (LPU) to ensure cases are progressed, sanctions applied and that redress is sought as appropriate.
- Ensuring that security incidents are publicised as appropriate and in accordance with NHS protect guidelines.
- Providing advice and guidance as required to the Trust.
- Producing an Annual Report and Annual work Plan.
• Liaising with NHS Protect and undertaking LSMS duties, including the provision of routine information to NHS protect, as required.

4.7 Heads of Service/Managers and Supervisors (with responsibility for Health, Safety, Security and the working Environment)

Heads of Service, Managers and Supervisors are responsible for leading on and promoting security, safe working practices within their areas of responsibility, in particular they will be responsible for:

• Ensuring that local procedures and protocols are developed for the security and safety of all persons, property, assets and information within their area of responsibility.
• Inform staff of Security Management Policy and ensure they are aware of local procedures and protocols and of their responsibilities for security.
• Ensure staff are issued with identification badges and wear/carry in accordance with local protocol.
• Ensure staff attend statutory and mandatory training.
• Report, review, manage and investigate security related incidents in line with Trust Policy, ensuring staff are aware of their responsibilities, and of the process, for incident reporting.
• Undertake and review periodically, or where required, inspections and risk assessments of all work activities and of all environments where their staff are required to work. This should include the physical security of premises and assets.
• Prepare action plans, and take appropriate action, to eliminate or minimise risk from hazards identified through the risk assessment process.
• Where required undertake lock down risk profiles for each of the sites.
• Managers should ensure staff are made aware of the Incident Reporting, Managing and Investigating Policy and that all incidents within their area of responsibility are reported in accordance with the policy.

4.8 Estates Manager

The Estates Manager is responsible for:

• The management of maintenance of Trust owned properties and security systems to maintain the physical security of premises.
• Ensuring that the physical security of premises and assets are considered in the planning of new developments and upgrading of existing buildings.

4.9 Head of Health, Safety and Security

The Head of Health, Safety and security supports the delivery of developed arrangements for the security management within
appropriate risk management systems identifying security issues relating to the Trust’s business premises.

4.10 Health & Safety Officers and Fire Safety Advisers

The Health & Safety Officers and Fire Safety Advisers give guidance to all managers on all matters affecting fire, health, safety & security.

Health and Safety Officers and Fire Safety Advisers support the management of Health, Safety & Security arrangements at Trust locations. The Health & Safety Officers support managers and supervisors in developing their Health, safety & security related risk assessments, procedures and protocols.

The effectiveness of local procedures are monitored via inspections, meetings, a review of risk assessments, audits, etc.

4.11 Staff

Staff are responsible for:

- Ensuring they have read and understand their responsibilities within the Security Management Policy.
- Complying with Trust wide and local procedures and protocols.
- Informing their manager of any actual or suspected security issues and reporting incidents in accordance with the Trust policy.
- Wearing or carrying identification badges in accordance with local protocols.

4.12 NHS Organisation Statutory Responsibilities

The Trust is committed to complying with all legislation and will undertake to maintain good practice at all times.

4.12.1 NHS Protect

NHS Protect, formerly known as NHS Counter Fraud and Security Management Service, has been the statutory body (under Secretary of State Directions SI 3039/2002) responsible for the management of security within the NHS since April 2003. From April 2012, their role is outlined in the NHS Standard Contract at section E37. NHS providers have a contractual duty to those who commission their services to meet the security requirements as set out in E37. In addition to this, NHS Protect has established processes with the Care Quality Commission with certain security functions forming part of the Quality Risk Profile (QRP) process.

4.12.2 Health & Safety Executive

The Health and Safety Executive (HSE) ensures that risks to staff’s health from work based activities are properly controlled and enforces
health and safety at Work Act 1974 to ensure as far as is reasonably practicable that the health, safety and welfare of employees and non-employees are not affected by work activities.

Management of Health and Safety at Work Regulations 1999: require employers to carry out risk assessments, make arrangements to implement necessary measures, appoint competent people and arrange for appropriate information and training.

### 4.12.3 Care Quality Commission (CQC)

The CQC is the independent regulator of health and adult social care services in England. As the regulator they ensure that an organization meets the government standards of quality and safety.

Outcome 10 (Regulation 15): Safety and Suitability of Premises requires organizations to ensure that service users and others having access to premises are protected against the risks associated with unsafe or unsuitable premises, by means of appropriate measures in relation to the security of the premises.

### 4.12.4 NHS Litigation Authority

The NHS Litigation Authority (NHSLA) has the statutory responsibility for the handling of negligence claims made against NHS bodies in England and has developed a single set of risk management standards to be met by all NHS Trusts i.e. NHSLA Risk Management Standards. The criteria for a Secure Environment, which the Security Policy reflects, is covered within these Risk Management Standards.

---

5. **Process**

5.1 **Policies**

The Trust has developed and implemented a number of policies which contribute to the delivery of the Trust Security Management strategic aims. For example:

- Risk Assessment Policy
- Incident Reporting Policy
- Lone Working Policy
- ID Badge Policy
- Violence and Aggression Management through Restrictive physical Interventions Policy

5.2 **Risk Management**

It will primarily be the responsibility of individual service/department/ward managers and team leaders to ensure that the risk assessment process is applied to security, violence and the working environment for
their areas of responsibility. Specialist and professional advice can be sought from the Safety & Quality department to assist with this process.

The identification, assessment and management of risks around security are the responsibility of every manager. Security risks will be identified following:

- An incident
- An occurrence
- Raised as an issue by staff or members of the public.

The risk should be recorded using a Risk Assessment Form. Where the risk has materialised into an incident, it should also be reported through the Trust’s incident reporting.

Assessments should be undertaken using the Trust Risk Assessment Form, which is available on the Trust Health and Safety Department Intranet site.

The process for completing a Risk Assessment is identified in points i to v. It is the responsibility of the manager, with support of staff members to complete the following steps as part of the Risk Assessment:

1. Identify hazards involved in manual handling within their area.
2. Identify the controls in place to address these.
3. Grade the risk using the Trust Risk Assessment Matrix.
4. Detail any further action required to address the risk.
5. Review the assessment at least annually or in the event of any incidents or significant changes.

Where action to address the risk has been identified, it is recorded on the Assessment Form which provides the manager and staff member with an action plan.

Managers are required to review the assessment periodically, but at least annually, to ensure actions are addressed and followed up.

5.3 Security Alerts

The NHS Protect operate a Security Alert system for anyone that has caused concern on any NHS premises anywhere in the country. These alerts are sent to Trusts to be drawn to the attention to the relevant wards or departments. Coventry & Warwickshire Partnership NHS Trust has in place a procedure for disseminating the alerts to the appropriate persons.
5.4 **General Reporting Procedures**

Once it has been identified that a breach of site security has occurred it is the responsibility of all Trust staff to ensure that the incident(s) is reported in line with Trust Incident Reporting Policy.

5.5 **Incident Review Procedures**

It shall be the responsibility of Heads of Service/Managers and Supervisors to ensure that the process of reviewing security related incidents (including incidents related to violence and/or aggression) is undertaken on a day to day basis to ensure that trends and impact factors are identified and to further ensure appropriate control measures are implemented to mitigate risks associated with such incidents. It shall also be the responsibility of Heads of Service/Managers and Supervisors to ensure any person who has been unduly affected by events pertaining to a security related incident(s) is given appropriate support and provided with appropriate information on all actions taken and the control measures that have been implemented following the reported incident(s). Specialist and professional advice can be sought from the Local Security Management Specialist to assist with this process.

5.6 **Violence and aggression (Physical & Non Physical Assault)**

It should be recognised that the management of violence and aggression will always present a significant risk to an organisation such as this Trust and due to the very nature of the client/patient base that care is delivered to, staff delivering such care can expect to have to manage challenging behaviour which will at times include the management of violence and/or aggression. It should also be recognised that The Trust is committed to ensure that relevant control measures are implemented to mitigate against identified risks related to violence and/or aggression and all staff receive the relevant training and have the relevant skills to be able to deal with such situations.

5.7 **Paediatric/Children Security**

The provision of a safe and secure environment is recognised by the trust as a statutory requirement of health and safety legislation and, in particular, compliance with the Secretary of State’s Directions to NHS Bodies on Security Management Measures.

Risk Management will be at the heart of Security Risk Management. The Trust will harness the information and experience of individuals within the Trust (and external expertise as appropriate) and translate that, with their help, into positive action which will either eliminate or reduce risks.
Services are responsible for carrying out suitable and sufficient risk assessments and where required develop local policies, protocols and procedures bringing them to the attention of all stakeholders. The risk Assessment process is detailed in the Trust Risk Assessment Policy.

The following policies are included on the Trust intranet:

- Admitting a Young Person to an Adult Ward Policy
- Children Visiting on Wards and Units
- Work experience and Volunteers Policy

5.8 Physical Security of Buildings, Premises and Assets

The Trust is committed to ensure that effective control measures and work practices are developed and maintained to enhance the physical security of all its buildings, premises and assets. The following information will detail procedural and operational directions to ensure this is achieved.

5.8.1 New Builds, Redevelopment or changes of use of existing premises

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

5.9 Access Control Systems and key Security

Where access control systems are utilised on Trust premises it shall be the responsibility of the designated Manager of the Ward, Unit or Department to ensure that local protocols are in place to ensure correct procedures and working practices are adopted for the use and management of such systems.

The following information shall provide guidance, direction and best practice to be adopted by staff where access control systems are utilised.

- Doors that are designated access control points (i.e. air lock door entry into restricted area) should be kept closed at all times and should never, for any reason, be propped open.
- Keys or access control proximity/swipe cards that have been allocated to an individual member of staff should never be loaned to, or used by another person.
• Staff should always be aware of, and safeguard against potential unauthorised access into restricted areas and not allow unauthorised persons attempting to tailgate through access control points into such areas.
• Premises and individual departments vacated for any length of time must be secured to restrict any form of unauthorised entry.
• Combinations for key pad control locks should never be given to unauthorised persons and should be changed at least twice a year.
• All access control points should be checked on a regular basis to ensure that they are working correctly and are properly secure.

5.9.1 Control of keys

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

• The issuing, recovery, recording and security of departmental keys are the responsibility of Ward/Unit/Departmental Managers.
• Staff should be aware of all procedures relating to their area of work for the issue, security and use of keys.
• Duplicate keys must be available in a designated secure place for use in the event of an emergency.
• Keys should not be able to be identified easily and should not be tagged with the name of Ward/Department/Site to which they belong. For example, colour coding is a secure method of identification providing the explanatory chart is stored separately from the keys themselves.
• Managers should keep a list of keys issued to staff and should ensure that they are returned prior to staff leaving.
• Managers need to consider whether to replace locks if keys are not returned.
• Contractors should only be given keys if the manager/estates department can guarantee adequate supervision and a record of their staff permitted to be on site. The list must be kept by the manager in case of subsequent burglaries.
• Lost/missing keys should be reported as incident using Trust incident reporting process

5.9.2 Staff & Visitor Identification

All staff and visitors shall adhere to the following directions and guidance with regards to Identification Systems whilst on Trust premises or Trust business: -

• Whilst on Trust business, all staff will have available on their person, at all times, a standard Trust ID Card.
• ID Cards will bear the Trust name, the individuals name & designation and photographic likeness of the individual.
• Lost or damaged cards must be reported to the individual's line manager immediately and a replacement sought without delay.
• ID Cards must be surrendered to the individual's line manager on leaving the employment of the Trust.
• Individual managers who employ or allow temporary workers, volunteers or contractors on their premises shall ensure that these persons are bona-fide and if these persons are working within the area for a considerable period of time then consideration should be given to issuing them with a Trust ID Card.
• Individual Wards/Departments/Units shall be encouraged to operate a 'visitor recording system' that requires all visitors to Trust premises to sign in/out of such premises.
• Visitor recording systems may vary between sites and areas but all should record similar information that will include – the visitor's name, the date, the purpose of their visit and the registration of any vehicle parked on the premises.
• All visitor recording systems will include reference to essential safety information that must be brought to the attention of the visitor on their arrival – i.e. action to be taken in event of fire or other emergency.

5.10 Alarm

5.10.1 Security Alarm Systems (Burglar Alarms)

Security alarm systems that are properly selected, correctly installed and properly monitored can help to prevent losses of property through criminal activity and provide better personal protection for staff and patients. It should however be recognised that an alarm system can only monitor areas for breaches in security and will not protect premises, objects or personnel by themselves. To offer protection, an effective response to the alarm activation is essential.

Where security alarm systems are utilised on Trust premises it shall be the responsibility of the designated Manager of the Ward, Unit or Department to ensure that local protocols are in place to ensure correct procedures and working practices are adopted for the use and management of such systems.

All staff who are required to use these systems during the course of their work should be given the relevant training and guidance to ensure that they are utilised in the correct manner.

5.10.2 Panic Alarm Systems

• In all high risk inpatient areas, staff will have the use of an effective panic alarm system. The requirement for a system will be made following a suitable risk assessment of the area by service manager.
• In line with The Provision and Use of Work Equipment Regulations 1992, it will be suitably and sufficiently maintained.
• It is recommend that as a minimum weekly panic alarm checks are made to ensure the continuous efficiency of the system.
• All managers must ensure that all staff receives an appropriate level of training in its use which is documented and regularly updated.
• It is true to say that the use of a panic alarm system is only as good as the procedure which backs it up. On this basis managers must ensure that robust procedures exist in terms of action to be taken in the event of activation and individual roles and responsibility.
• A system for monitoring the effectiveness of the procedure must be included in any local procedure.
• A post-incident analysis following alarm activation or failure to activate can provide valuable information in order that lessons can be learnt to improve procedures.

5.10.3 Personal Alarms

In areas not covered by integral panic alarm systems, staff may feel access to a personal attack alarm is beneficial.

Lone working risk assessments undertaken by the manager will highlight if and where a personal alarm should be issued to the staff member. This will be based on the level of risk to staff health, safety & security.

5.11 Closed Circuit Television (CCTV)

The Trust operates a number of CCTV systems across the organisation at different locations and premises. These systems are operated normally independently on a day to day basis by the reception staff for the area that the systems are in operation. Most CCTV images are not routinely monitored by Trust staff and systems are mainly used retrospectively to retrieve stored images where it has been identified that a crime or breach of security has occurred and evidence is required as part of the investigative process.

The following information will detail legislative guidance and direction on the use of CCTV systems by the Trust.

• All CCTV systems operated by the Trust shall be done so in accordance with legislative direction and codes of practice in relation to the following:
  • The Data Protection Act 1998.
  • The Human Rights Act 1998.
  • The Information Commissioner’s Office (ICO) CCTV Code of Practice 2008.
• An area that operates CCTV for, or on behalf of, the Trust shall have in place local protocol for the usage and operation of the system.
• That any CCTV system is not abused or misused
• That CCTV is correctly and efficiently installed, monitored and operated.
• The SMD shall be the appointed person by the Trust as the appropriate Director who has overall legal responsibility for CCTV systems operated by the Trust.
• All staff involved in the operation or monitoring of CCTV systems operated by the Trust have a responsibility to comply with associated legislation and guidance.
• The LSMS shall have an oversight of procedures supporting the operational use of CCTV systems utilised by the Trust to ensure compliance with legislation and guidance and provide the SMD assurance that relevant requirements are being met.

5.12 Security of Property (Trust/Patient /Personal)

The Trust is committed to ensure that effective control measures are in place to ensure that Trust, patient or personal property is not subject to theft, loss, malicious/criminal damage or misuse. The following information shall detail direction and guidelines to ensure this is achieved.

5.12.1 Trust Property

It is the responsibility of all Managers to ensure a comprehensive inventory of all Trust equipment is maintained for their area of responsibility and kept up to date as appropriate. Equipment moved between premises and departments should be always recorded in and out as appropriate and a register and/or written record of such movement of property should be maintained at a local level.

Equipment capitalised under the Trust’s accounting policies should always be included in the Trust’s Asset Register operated by the Director of Finance. All Managers have a responsibility to co-operate with the Director of Finance to ensure that the Asset Register is complete, accurate and timely.

Staff should ensure adequate measures are taken to protect Trust equipment and that all items of equipment are not left vulnerable to potential theft, loss, malicious/criminal damage or misuse.

When Trust equipment is not in use all items should be stored in a secure environment and not left on general view. When Trust equipment is carried in vehicles it should always be safeguarded by placing items out of sight and locking the vehicle when unattended. All incidents of theft, loss, malicious/criminal damage and misuse of Trust equipment should be reported through Incident reporting process.
5.12.2 Patient Property (Wards & Residential settings)

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

- Record all property that is formally handed over and ensure the patient is issued with a receipt.
- To advise patients and their relatives/carers of the risks if they do not formally hand property over for safekeeping.
- A patient’s property form must always be completed even if patients do not hand over property.
- If patients are likely to be away from the Ward/Unit for a period of time, staff must encourage them to hand over all valuables for safekeeping.
- Individual Directorates must develop processes for the recording of all patient property brought into wards and/or units.

5.12.3 Staff Property

All staff must take responsibility for their personal property and to make use of locked facilities where available. Only essential items and minimum quantities of cash should be brought to work. Staff should not leave valuable items unattended at any time. The Trust does not take responsibility for losses of or damage to personal property at work.

5.13 Security of Drugs, prescription forms and hazardous material

The Strategy for safe and secure handling of drugs, controlled prescription stationary and disposal of pharmaceutical waste is handled via the Medicines Management Team

5.14 Lockdown (Emergency Procedures)

In line with its responsibility to ensure a safe and secure environment, the NHS Security Management Service has developed guidance to explain the planning and execution of a lockdown in NHS healthcare sites, which will usually be either primary or secondary care Trusts in England.

The Trust will develop plans and procedures based on such guidance to achieve hospital lockdown: to prevent freedom of entry/exit and movement to a site or other specific Trust building or 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 a Trust facility to operate.

**Defining site/building lockdown**

A lockdown is the process of preventing freedom of entry to, exit from or movement within the Trust. In this way, the Trust can either contain or exclude staff, patients or visitors. Supporting the overarching objective of excluding or containing staff, patients or visitors, a lockdown may be characterised as a partial (static or portable), progressive or full lockdown.

- **Partial Lockdown** – the locking down of a specific part of the Trust, or a specific building or part of a building. Partial Lockdown can also be defined as the application of entry restrictions within a specific area to control the flow of people into it.
- **Progressive Lockdown** – a step-by-step Lockdown of a location or building in response to an escalating incident. The Trust and should be able to systematically expand the lockdown procedure across a wide range of buildings or areas.
- **Full Lockdown** – characterised by preventing entry or exit for an entire Trust site or building.

The production of the Lockdown Risk Profiles will be lead by the relevant Local Security Management Specialist in conjunction with Directorate Management Teams and Facilities and Estates.

It is vital to ensure engagement with the appropriate stakeholders during the development of a lockdown risk profile. In order to ensure that all implications of implementing a lockdown have been considered a multidisciplinary approach should be taken which should include external stakeholder involvement e.g. the Police, Ambulance and the Local Authority.

**5.15 Major Incidents and Contingency Planning**

The Civil Contingencies Act 2004 is important legislation providing a statutory and regulatory framework for resilience in the UK. The act delivers a single framework for civil protection in the UK and sets out clear expectations and responsibilities for front-line responders at the local level, to ensure that they are prepared to deal effectively with the full range of emergencies from localised incidents to full-scale emergencies.

The Civil Contingencies Act (2004) and accompanying regulations and guidance provides a single framework for civil protection across the United Kingdom. The Act (CCA) is divided into two parts:

**Part 1** - focuses on local arrangements for civil protection, establishing a statutory framework of roles and responsibilities for local responders.
Part 2 – focuses on emergency powers, establishing a modern framework for the use of special legislative measures that might be necessary to deal with the effects of the most serious emergencies.

RESPONDERS

Two types of responders have been identified, these are:

**Category 1 Responders** are those organisations at the core of any emergency response; for example local authorities, the emergency services, Primary Care Trusts, NHS Trusts and NHS Foundation Trusts with accident/emergency facilities, Ambulance Service NHS Trusts, and the Health Protection Agency.

**Category 2 Responders** are those organisations likely to be heavily involved in any emergency response, for example utility companies (water, gas, electricity, telecommunications), rail companies, airport operators, the Highways Agency, Strategic Health Authorities.

5.16 Suspect Packages/Suspicious behaviour

All staff should remain vigilant and be on the look out for unusual or suspicious behaviour. If it has been noted that there are unexpected visitors in restricted parts of the building or that a package or object has been placed in an unlikely spot, then there should be an immediate response. However minor if there is a suspicion that there is potential danger to the staff and visitors on site, then the site manager should be alerted and a prompt response to the situation initiated. If the risk to safety is such that there should be an immediate evacuation then the local evacuation plan should be activated. An emergency call should be made to the Police and lockdown initiated (see 6.2). The evidence at the scene will need to be preserved to support follow up investigations. The police approach in the event of a potential bomb scare is summarised as the 5 C’s: Confirm - from a safe distance, Clear area - keeping away from the device, Cordon the area, Control Access - do not allow anyone near, Check - for secondary hazards or devices.

5.17 Audit

The Health, Safety & Security function carries out annual audits with each service on annually basis. The audits carried include premises and Lone Working. An audit form has been designed and used for each audit to ensure consistence.

5.18 Prevent (Counter Terrorism)

CONTEST, the UK’s Counter-terrorism strategy, aims to reduce the risk to the United Kingdom and its interests overseas from terrorism, so that people can go about their lives freely and with confidence.
CONTEST is organised around four principal work streams:

- **Pursue**: to stop terrorist attacks.
- **Prevent**: to stop people from becoming terrorists or supporting terrorism.
- **Protect**: to strengthen our protection against terrorist attacks.
- **Prepare**: where an attack cannot be stopped, to mitigate its impact.

The Trust’s contribution to the Prevent work stream is to categorise Prevent as Statutory and Mandatory training therefore all staff attending Induction and the Statutory & Mandatory training will receive the Prevent training.

The Prevent initiative is led by the Trust’s Safeguarding Children and Vulnerable Adults function. If staff are concerned that vulnerable individuals are being exploited/radicalised for terrorist-related activities, they must follow the guidance in Appendix 3.

As well as following the guidance in Appendix 3, Staff must inform the Safeguarding Team.

6. **Consultation**

This policy has been developed in consultation with managers and staff via the Health, Safety and Security Committee. All Trust staff have had the opportunity to comment via consultation on the Intranet.

7. **Implementation**

Managers are responsible for the implementation of this policy in their areas of responsibility.

8. **Training and Support**

The annual process for identification of training needs will provide information on what security training is required by each service. However other Mandatory training packages do cover certain aspects of training which contribute to the security management aims of the Trust. The Trust’s Training Brochure outlines available training and the Health Safety & Security Team can provide additional advice and guidance.

The Trust will ensure that sufficient training is provided for its staff to manage security related incidents. This will be achieved by an introduction to security within the Trust induction programme and when requested by services.
9. Review

This policy will be reviewed at least every three years by the Policy Author.

10. Monitoring Compliance

<table>
<thead>
<tr>
<th>Aspect of compliance or effectiveness being monitored</th>
<th>Monitoring method</th>
<th>Individual department responsible for the monitoring</th>
<th>Frequency of the monitoring activity</th>
<th>Group/committee which will receive the findings/monitoring report</th>
<th>Group/committee/individual responsible for ensuring that the actions are completed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duties</td>
<td>Review of policy every 3 years</td>
<td>Head of Health &amp; Safety</td>
<td>3 yearly</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Monitoring of the risk assessments, including action plans and follow up, for the physical security of premises and assets</td>
<td>Security Audit</td>
<td>LSMS</td>
<td>Annual</td>
<td>Health, Safety and security Committee</td>
<td>Operational Manager</td>
</tr>
</tbody>
</table>

11. References

- Tackling crime against the NHS – a strategic approach
- Standards for Providers – Security Management
- **Tackling violence and antisocial behaviour in the NHS Joint Working Agreement between the Association of Chief Police Officers, the Crown Prosecution Service and NHS Protect**
- A Professional Approach to Managing Security In the NHS – Counter Fraud and Security Management Service (December 2003)
- Security Management Service extranet site – LSMS security manual
- Secretary of State for Health Directions; 2003 Directions to NHS Bodies on measures to deal with violence against NHS staff. (As Amended 2005). 2004 Directions on NHS Security Management Measures (As Amended 2005)
- ‘Tackling violence against staff’ - explanatory notes for reporting procedures by Secretary of State Directions in November 2003 (Updated June 2009)
- Non Physical Assault SA8 (NHS Protect)
- National Health Service Litigation Authority (2007)
- Health and Safety Law – Health and Safety Executive (October 1999)
- Health & Safety at Work etc Act 1974
• Children’s Act 1989. Police Act 1997 part V
• Data Protection Act 1988
• Private Security Act 2001
• Guidance in support of functional provisions for healthcare premises. The Regulatory Reform (Fire Safety) Order 2005
• Health Technical Memorandum 05-02
• Building Partnerships, Staying Safe – The health sector contribution to HM Government’s Prevent Strategy: Guidance for healthcare organisations

12. **Trust Associated Documents**

• Health and Safety Policy, CWPT
• Incident Reporting, Managing and Investigating Policy, CWPT
• Standing Financial Instructions and Standing Orders, CWPT
• Whistle Blowing Policy, CWPT
• Risk Assessment Policy, CWPT
• Management of Violence and Aggression through Positive Behavioural Approaches &Restrictive Physical Intervention, CWPT
• Lone Working Policy, CWPT
• COSHH Policy, CWPT
• Fire Safety Policy, CWPT
• Admitting a Young Person to an Adult Ward Policy
• Children Visiting on Wards and Units
• Work experience and Volunteers Policy
• Sexual Safety In Patient Settings

13. **Version Control**

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Author</th>
<th>Status</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>V1.0</td>
<td>17/2/09</td>
<td>Martin Harrop LSMS</td>
<td>Draft</td>
<td>Original draft text</td>
</tr>
<tr>
<td>V2.0</td>
<td>19/2/09</td>
<td>Martin Harrop LSMS</td>
<td>Draft</td>
<td>Changes following Health and Safety meeting</td>
</tr>
<tr>
<td>V3.0</td>
<td>20/2/09</td>
<td>Martin Harrop LSMS</td>
<td>Draft</td>
<td>Final draft for submission to staff side for consultation</td>
</tr>
<tr>
<td>V4.0</td>
<td>20/3/09</td>
<td>Martin Harrop LSMS</td>
<td>Approved</td>
<td>Safety and Quality Committee</td>
</tr>
<tr>
<td>V4.1</td>
<td>4/11/10</td>
<td>Becky Keough NHSLA Co-ordinator</td>
<td>Draft</td>
<td>Format changes</td>
</tr>
<tr>
<td>Version</td>
<td>Date</td>
<td>Author/Enhancer</td>
<td>Status</td>
<td>Content/Reason</td>
</tr>
<tr>
<td>---------</td>
<td>------------</td>
<td>-----------------</td>
<td>--------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>V4.2</td>
<td>30/11/10</td>
<td>Martin Harrop LSMS</td>
<td>Draft</td>
<td>Content changes to include lockdown</td>
</tr>
<tr>
<td>V4.3</td>
<td>17-2-11</td>
<td>Becky Keough NHSLA Co-ordinator</td>
<td>Approved</td>
<td>Policy Review Group amendments</td>
</tr>
<tr>
<td>V4.4</td>
<td>24-10-2012</td>
<td>Darrell Linton Local Security Management Specialist</td>
<td>Draft</td>
<td>Harmonisation with CCHS policy, NHSLA compliance and NHS Protect Security template</td>
</tr>
</tbody>
</table>
14. Equality Impact Assessment

**DOCUMENT/PROJECT NAME:** Security Management Policy

<table>
<thead>
<tr>
<th>Yes/No</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. **Does the document affect one group less or more favourably than another on the basis of:**
   - Race: No
   - Human Rights: No
   - Gender (inc gender reassignment): No
   - Religion or Belief: No
   - Sexual Orientation: No
   - Age: No
   - Disability (learning disabilities, physical disability, sensory impairment and mental health): No

2. **Is there any evidence that some groups are affected differently?**
   - No

3. **If you have identified potential discrimination are there any expectations valid, legal and/or justifiable?**
   - 

4. **Is the impact of the document/guidance likely to be negative?**
   - 

5. **If so, can the impact be avoided?**
   - 

6. **What alternative is there to achieving the document/guidance without the impact?**
   - 

7. **Can we reduce the impact by taking different actions?**
   - 

8. **How has the consultation taken place and who with?**
   - Who with: Via Trust consultation policy

9. **EIA Team:** 3 people who contributed to this assessment
   - 1. Malcolm Norton - Head of Health and Safety
   - 2. Victoria Brownsword – Risk Coordinator
   - 3. Darrell Linton – Local Security Management Specialist

10. **Date of the Assessment:**
    - 12 February 2013

If you have identified a potential discriminatory impact on this procedural document, please refer it to the author/Lead, together with any suggestions as to the action required to avoid/reduce this impact. For advice in respect of answering the above questions, please refer to the EIA guidance notes on the Equality and Diversity Intranet Page.

**Please return to the Equality and Diversity Department**
Appendix 1

Boards, Committees and Forum
Appendix 2

NHS Protect

NHS Protect was launched in April 2011 as an intelligence-led, stakeholder focused service. Its purpose is to safeguard NHS resources. NHS Protect leads on work to identify and tackle crime across the health service. The aim is to protect NHS staff and resources from activities that would otherwise undermine their effectiveness and their ability to meet the needs of patients and professionals. Ultimately, this helps to ensure the proper use of valuable NHS resources and a safer, more secure environment in which to deliver and receive care.

The document ‘Tackling crime against the NHS – A strategic approach (see NHS Protect website) outlines NHS Protects Strategy for tackling crime in the NHS.

NHS Protect has five strategic aims:

- To provide national leadership for all NHS anti-crime work.
- To work in partnership with the Department of Health, commissioners and providers, as well as key stakeholders, such as the police and crime prosecution service, local authorities, etc.
- To establish a safe and secure environment that has systems and policies in place.
- To lead, within a clear professional and ethical framework, investigations.
- To quality assure the delivery of anti-crime work with stakeholders to ensure the highest standard is consistently applied.

These aims will be met by working in accordance with the following three key principles for action, which underpin all anti-crime work in the NHS.

These principles apply across the sector, at national and local and at strategic and operation level.

The three key principles are:

- Inform and involve those who work for or use the NHS about crime and how to tackle it.
- Prevent and Deter crime in the NHS to take away the opportunity for crime to occur or re-occur and discourage those individuals who may be tempted to commit crime.
- Hold to account those who have committed crime against the NHS.

NHS Protect has developed standards, which provide a more detailed framework of requirements that apply to organisations involved in the delivery of NHS care. These standards, which are available on the NHS Protect website, give more detail on what is expected at a local level when implementing this strategy and working in accordance with the key principles of action.
NHS Protect will quality assure anti-crime work across the NHS by monitoring compliance against the standards and assessing the quality of the anti-crime work carried out across the sector.
Appendix 3

Reporting Flowchart for Raising Concerns

Action to take if you suspect an individual is being radicalised/self-radicalised into extremist activities

Is the person (child or adult)

At immediate risk

Is the person indicating/showing behaviour that indicate they are likely to be an immediate risk of initiating a violent extremist attack

Yes

Contact Police and ask for Specialist Counter Terrorism Unit

Contact 999 and request police presence

(Complete an incident form)

Causing Concern

No

There is no immediate risk but you have a concern that someone is vulnerable/susceptible to being led into extremist activities

PG/JH Prevent August 2012