Security Policy

<table>
<thead>
<tr>
<th>Version Number</th>
<th>4.1</th>
<th>Version Date</th>
<th>August 2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Owner</td>
<td>Chief Financial and Commercial Officer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Author</td>
<td>Facilities Manager</td>
<td></td>
<td></td>
</tr>
<tr>
<td>First approval or date last reviewed</td>
<td>Aug 2009, October 2011 (Version 4)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Staff/Groups Consulted</td>
<td>Security Committee  Health and Safety Committee  Local Security Management Specialist  Trust Risk Manager  Heads of Departments  Chief Pharmacists</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Discussed by Policy Group</td>
<td>October 2011</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Approved by HMT</td>
<td>1 November 2011</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Next Review Due</td>
<td>August 2016</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Equality Impact Assessment Completed</td>
<td>August 2013</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Table of Contents

1. Rationale .................................................................................................................. 3
2. Policy Statement........................................................................................................ 3
3. Applicability ............................................................................................................... 3
4. Policy Provisions ...................................................................................................... 3
4.1 Risk Assessment Process ...................................................................................... 3
4.2 Incident Reporting .................................................................................................. 4
4.3 Major Incidents, Contingency Planning and Lockdown Procedure ..................... 4
4.4 Security Department ............................................................................................. 4
4.5 Closed Circuit Television (CCTV) ........................................................................ 4
4.6 Terrorist Threats ..................................................................................................... 5
4.7 Training .................................................................................................................. 5
5. Associated Procedures ............................................................................................... 6
6. Implementation, Monitoring and Evaluation ............................................................. 6
7. Definitions ................................................................................................................ 6
7.1 NHS Protect ........................................................................................................... 6
7.2 Lockdown ............................................................................................................... 6
7.3 Lockdown risk profile ............................................................................................ 6
7.4 Bomb (Improvised Explosive Devices) ................................................................. 6
7.5 Security Incident .................................................................................................... 7
7.6 Lone Working ........................................................................................................ 7
7.7 Closed-circuit Television .................................................................................... 7
8. Table of Roles and Responsibilities ........................................................................ 7
9. Reference to other Policies ....................................................................................... 8
10. Source References and Acknowledgements ............................................................ 8
Annex A – Equality Impact Assessment Tool ................................................................. 9
1. **RATIONALE**
The purpose of the Security Policy is to establish and maintain robust structures and processes to manage the security of patients, visitors, staff and the Trust’s premises and assets. All NHS Staff deserve the right to work in a safe & respectful environment without fear of violence, aggression, abuse or harassment from patients & relatives.

2. **POLICY STATEMENT**
The aim of the Security Policy is to set out the responsibilities for arrangements that protect, deter, report and educate as part of a comprehensive security management environment.

The Trust follows the NHS Protect security management strategy for the NHS laid out in the NHS Protect document *‘A professional approach to managing security in the NHS’*. This strategy has six strands which are:

- Deterring
- Preventing
- Detecting
- Investigating
- Sanctions
- Redress

3. **APPLICABILITY**
This Policy applies to all permanent and temporary staff, and Contractors employed by Yeovil District Hospital NHS Foundation Trust. Failure to follow this policy by staff may result in action under either the Disciplinary or Capability policies. Other persons may be subject to other action by the Trust.

4. **POLICY PROVISIONS**

4.1 **Risk Assessment Process**

4.1.1 **Departmental Review**
All departments must have a Security Risk Assessment of their workplaces. The Security Risk Assessment template held by the Security Department should be completed by the department manager. Guidance is available from the Local Security Management Specialist (LSMS).

The aim of the risk assessment is to identify the risks associated with:

- the physical security of premises and assets.
- potential threats from violence and aggression.
- lone working in the department.

The assessment must establish what control measures are in place and evaluate the effectiveness of those control measures. It must also plan and implement any new control measures required. To support this incident reports will be reviewed to identify at risks areas.

The risk assessment must be maintained as a live document to be reviewed by the department manager at least annually, when a security incident occurs or when physical changes occur to the department.

4.1.2 **Risk Assessment monitoring**
The Local Security Management Specialist will maintain an overall central register of security risks assessments conducted and actions identified and progress on implementation. A report will be submitted to the Security Committee on a quarterly basis. Progress on actions to mitigate risk will be monitored by the committee using these quarterly reports.
4.2 Incident Reporting
All staff within the Trust have access to ‘Safeguard’, the Trust’s incident reporting system, through the intranet. ‘Safeguard’ is linked to the NHS Protect Security Incident Reporting System (SIRS), and all security related incidents are automatically uploaded into the system from ‘Safeguard’ through the Trust incident reporting lead.

A detailed report of security incidents is submitted to the Security Committee at each meeting. The committee assess Trust-wide trends and initiates the necessary action to ensure future risks are minimised.

4.3 Major Incidents, Contingency Planning and Lockdown Procedure
The Trust has a Major Incident Response Plan and a Business Continuity Policy. As part of these plans the Trust is required to have a Lockdown Risk Profile and procedures in place. A lockdown may be required in response to a specific incident, or as a proactive measure in response to receiving specific intelligence data, for example in connection with a terrorist threat.

A lockdown is achieved when access/egress into a department or building is controlled and restricted, this is achieved through a combination of physical security measures and the deployment of security personnel.

4.4 Security Department
The Security Department, managed by the Facilities Manager, will ensure arrangements are in place for the security of persons, premises and assets at all times. This may be done by agreeing contracts for the provision of security guards. The effectiveness and value of these arrangements will be subject to review by the Security Committee.

In addition to this, the Security Department will provide a specialised management service to the Trust that will include the following:

- The effective management of CCTV (and other technical security methods) in accordance with current legislation and best practice.
- The delivery of security awareness training to all staff as part of the Induction and Mandatory Training programme.
- Investigating and reporting on criminal activities throughout the Trust.
- Providing advice and guidance on security matters and lone working.
- Assessing security risks within departments and wards, and producing Security Risk Assessments, and action plans to mitigate the risks.
- Liaising with local police on crime reduction measures and with other relevant agencies on security/policing matters.
- Conducting security visits and inspections to review department security to support risk assessment findings.

4.5 Closed Circuit Television (CCTV)
The overall purpose of CCTV schemes is to help reduce the fear of crime for the Trust staff and service users / carers (particularly those who are entering and leaving the Trust premises during the hours of darkness) and to protect the Trust premises from criminal activities. They will also on occasions following risk assessment be used to enhance the security of service users within in-patient areas, monitoring access to bathroom and bed areas. The particular purposes of all schemes unless specifically identified as directed monitoring are in accordance with the following rationale:

- To assist in the prevention and detection of crime against both persons and property.
- To facilitate the identification, apprehension and prosecution of offenders in relation to crime.
- To ensure the security of property belonging to Trust and to employees and visitors of the Trust.

- All associated information, documents, and recordings obtained by CCTV are held and used in accordance with the Data Protection Act.

- Images obtained from CCTV recordings will not be used for any commercial purpose. Recordings will only be released to the media for use in investigation of a specific crime and with the written consent of the Police. Recordings will not be released to the media for purposes of entertainment.

- Archived CCTV images will not be kept for longer than is necessary for the purpose of Police evidence. Once there is no longer a need to keep the CCTV images, they will be destroyed as confidential waste.

- All associated information, documents, and recordings obtained and used by CCTV are protected by the Data Protection Act.

- Cameras monitor activities on Trust premises, car parks and other public areas to identify criminal activity whether occurring, anticipated, or perceived in order to enhance the safety and well-being of staff, patients, and visitors. All Security Officers are/have been made aware of this requirement.

- Except when specifically authorised by the NHS Protect, using specific Directed Surveillance as stipulated in the Regulation of Investigatory Power Act 2000 (RIPA), staff must not direct cameras at an individual, their property, or a specific group of individuals.

- The planning and design of CCTV systems has endeavoured to ensure maximum effectiveness and efficiency but cannot guarantee to cover or detect every incident occurring within the areas covered.

- Warning signs, as required by the Code of Practice of the Information Commissioner are displayed at all access routes to areas covered by the Hospital CCTV.

4.6 **Terrorist Threats**

The likelihood of a terrorist attack is considered to be extremely low.

A bomb threat procedure is to be drawn up in discussion with the Security Management Director, Local Security Management Specialist, Counter Terrorist Support Officers, Trust Risk Manager and local police, fire and ambulance. The Security Management Director must balance the potential risk to staff and patients against practical considerations, taking into account the advice from medial staff, the Police and other relevant agencies.

4.6.1 **Report of a Bomb Threat**

Should a bomb threat be received, the internally-activated element of the Major Incident Plan should be followed. If a decision is made to evacuate the building, the following procedures should be observed:

- Leave doors and windows open wherever possible.
- Leave lights on to assist in a subsequent search.
- Shut down any plant or machinery where possible.

4.7 **Training**

All staff joining the Trust are required to attend Induction Training. As part of the course, they must attend Security Awareness and An Introduction to Conflict Resolution. All staff must complete mandatory training every 2 years which includes both Security Awareness and An Introduction to Conflict Resolution training as a refresher.
For all areas where the risk assessment process has identified a high risk of conflict occurring are required to attend Conflict Resolution Training which follows the NHS Protect National Syllabus. Courses are to be arranged through the Yeovil Academy.

5. ASSOCIATED PROCEDURES
The Security Access Procedures provide details on access around the site. These are produced by the Facilities Manager and approved by the Security Committee. The Security Access Procedures can be accessed on the Security page on the Estates and Facilities intranet site.

The CCTV Management Procedures provide a management framework to safeguard the integrity of the Trust CCTV System, whilst ensuring the right to privacy is not breached. These are written by the Facilities Manager, and approved by the Security Committee. The CCTV Management Procedures can be accessed on the Security page on the Estates and Facilities intranet site.

The Major Incident Plan details the processes that are followed when an external or internal major incident is declared. A security incident may lead to a major incident being declared. The Major Incident Plan is written by the Head of Operations, and can be accessed on the Trust’s intranet site.

6. IMPLEMENTATION, MONITORING AND EVALUATION
Responsibility for implementation, monitoring and evaluation is identified in the Trust’s Policy on Procedural Documents.

The policy will be monitored by the Security Committee who will review all incidents and actions resulting from the incidents, review security risk assessments including lone worker arrangements and monitor the completion of the required actions to mitigate risk through annual audit by the Local Security Management Specialist. The audit will include the review of arrangements put in place to manage physical security, premises and assets, including the risk assessments for the prevention and management of violence and aggression. The Security Committee will receive a bi-annual report from the Local Security Management Specialist with the key findings and recommendations.

7. DEFINITIONS

7.1 NHS Protect
NHS Protect provides advice and guidance on policy and operational matters related to the management of security in the NHS.

7.2 Lockdown
Lockdown is the process of controlling the movement and access – both entry and exit – of people to all or part of the premises in response to an identified risk, threat or hazard that might impact upon the security of patients, staff and assets or indeed the capacity of that facility to continue to operate.

7.3 Lockdown risk profile
A Lockdown Risk Profile is a risk assessment of each site to determine its potential vulnerability to threat and its capability of either partial or full lockdown.

7.4 Bomb (Improvised Explosive Devices)
For the purposes of this policy these two terms are synonymous and refer to any actual or suspected explosive device. The popular term Bomb will be used in this policy.
7.5 **Security Incident**
Circumstance is which some or all of the processes referred to in this policy are activated to protect those present or near the Trusts premises. All such incidents should be reported in accordance with the Trust’s Incident Reports and Investigation Policy and Procedure.

7.6 **Lone Working**
Lone working is any situation or location in which a member of staff works without a colleague.

7.7 **Closed-circuit Television**
Closed-circuit television (CCTV) is the use of video cameras to transmit a signal to a specific, limited set of monitors. It differs from broadcast television in that the signal is not openly transmitted.

8. **TABLE OF ROLES AND RESPONSIBILITIES**

<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chief Executive</td>
<td>The Chief Executive has ultimate responsibility for ensuring the provision of a safe and secure environment for all staff, patients, visitors and contractors. The Chief Executive is responsible for nominating a Security Management Director (SMD).</td>
</tr>
<tr>
<td>Security Management Director</td>
<td>The SMD is the nominated Board lead for the Trust. The SMD is responsible for reporting on security matter to the Board of Directors and for ensuring the implementation of this policy.</td>
</tr>
<tr>
<td>Facilities Manager</td>
<td>The Facilities Manager is responsible for the operational implementation of the security policy. This includes line management of the Local Security Management Specialist and responsibility for the Security Guarding contract.</td>
</tr>
<tr>
<td>Local Security Management Specialist</td>
<td>The Trust shall appoint an accredited Local Security Management Specialist (LSMS), reporting to the SMD to act as the Trust security advisor. The role of LSMS is to work on behalf of the Trust to deliver an environment that is safe and secure so that the highest standards of clinical care can be made available to patients. Annually the LSMS will compile a report for the Trust Board detailing the work that has been carried out the previous year and each year will identify what actions the LSMS will employ to reduce security risks for the forthcoming year.</td>
</tr>
<tr>
<td>Security Committee</td>
<td>The membership of the Security Committee will be a wide representative group from the Trust, and will be chaired by the Director of Estates and Facilities. The Chair will report to the SMD who is the reporting lead to the Hospital Management Team and Board of Directors. Refer to the Terms of Reference for the Security Committee.</td>
</tr>
</tbody>
</table>
| Heads of Departments and Managers | Heads of Departments and Managers are responsible for the security of their workplaces, their staff and of any patients, visitors and contractors within their department. They must ensure:  
• All unoccupied areas are secured when not in use  
• Expensive equipment or hazardous materials are secured when not in use  
• Confidential documents are secured when not in use  
• Breaches of security are reported through the Trust’s incident reporting procedure. |
Criminal activity is reported to the police and through incident reporting procedures.

Security risk assessments are completed for each department/ward they are responsible for.

The risk assessment is held within the department and shared with the rest of the department where any security risks and actions have been identified.

Department staff are made aware of the security policy and any local procedures

Ward managers are to ensure that each patient’s property is managed in line with the Patients Property policy.

All staff

All staff are responsible for:

- Maintaining a secure environment for their colleagues, patients and visitors and to ensure wherever possible the protection of the premises and assets of the Trust.
- Being responsible for the security of their own personal property whilst at work.
- Challenging anyone that should not have access to an area of the premises or who is acting suspiciously.
- Wearing identity badges whilst at work.
- Ensuring security of access codes and keys in their possession.
- Reporting all security incidents through the incident reporting procedure.
- Ensuring that when they leave their place of work for any period of time it is secured.

9. REFERENCE TO OTHER POLICIES

This policy should be read in conjunction with the Managing Violence, Aggression and Abuse in the Workplace policy, the Incident Reporting and Investigation Policy and the Health and Safety Policy.

10. SOURCE REFERENCES AND ACKNOWLEDGEMENTS

- Data Protection Act 1998
- Health and Safety at Work Act 1974
- Human Rights Act 1998
- Secretary of State for Health’s Directions on NHS Security Management Measures (2003)
- Secretary of State for Health’s Directions on work to tackle violence against staff and professionals who work to provide services for the NHS (2003)
- Statutory Instrument 3039/2002
- NHS Protect Non-Physical Assault Explanatory Notes (2004)
- NHS Protect Tackling Violence Against Staff: Explanatory notes for reporting procedures introduced by Secretary of State Directions in November 2003 (2007)
- NHS Protect Conflict Resolution Training Implementing the National Syllabus (2004)
- The NHS Litigation Authority (NHSLA) Risk Management Standards for Acute Trusts (2011)
# ANNEX A – EQUALITY IMPACT ASSESSMENT TOOL

To be completed and attached to any procedural document when submitted to the appropriate committee for consideration and approval.

<table>
<thead>
<tr>
<th></th>
<th>Yes / No / N/A</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Does the policy/guidance affect one group less or more favourably than another on the basis of:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Race</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Ethnic origins (including gypsies and travellers)</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Nationality</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Gender</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Culture</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Religion or belief</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Sexual orientation including lesbian, gay and bisexual people</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Age</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Disability</td>
<td>No</td>
</tr>
<tr>
<td>2. Is there any evidence that some groups are affected differently?</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>3. If you have identified potential discrimination, are any exceptions valid, legal and/or justifiable?</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>4. Is the impact of the policy/guidance likely to be negative?</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>5. If so can the impact be avoided?</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>6. What alternatives are there to achieving the policy/guidance without the impact?</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>7. Can we reduce the impact by taking different action?</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>

If you have identified a potential discriminatory impact of this procedural document, please refer it to the Trust’s lead for Equality & Diversity, together with any suggestions as to the action required to avoid / reduce this impact.

For advice in respect of answering the above questions, please contact the Trust’s lead for Equality & Diversity.

Signed – Philip Watson  
Date: August 2013