# POLICY CONTROL SHEET

*(updated August 2011)*

| | | | | |
|---|---|---|---|---|
| Policy Title and ID number: | **Secure Environment Policy SE3.1** | | | |
| Sponsoring Director: | **Chief Operating Officer** | | | |
| Implementation Lead: | Lorraine Christopher | | | |
| Impact: | *(a) To patients* | **Yes** | | |
| | *(b) To Staff* | **Yes** | | |
| | *(c) Financial* | **Yes** | | |
| | *(d) Equality Impact Assessment (EIA)* | Completed: **Yes** | | |
| | *(e) Counter Fraud assessed* | Completed: **Yes** | | |
| | *(e) Other* | | | |
| Training implications: | *To be incorporated into induction:* **Yes / No** | | | |

| Date of consultation: | ***Approval Process*** | **Date** | **Local Consultation** | **Date** |
|---|---|---|---|---|
| | *Executive Team* | | *Joint Partnership Forum* | |
| | *Board Committee:* | | *Local Negotiating Committee* | |
| | • *Clinical Governance* | | *Infection Control Committee:* | |
| | • *Non Clinical Governance & Risk* | *17/01/12* | *Health & Safety Committee* | |
| | • *Audit Committee* | | *Quality Safety Improvements & Effectiveness Board* | |
| | • *Finance Committee* | | | |
| | • *RATS* | | *Investment Board* | |
| | *Trust Board Approval / Ratification* | | *Patients Experience Board* | |
| | *Other:* | | *Other:* | |
| | | | | |
| | | | | |
| | | | | |

| | | | |
|---|---|---|---|
| Approval/Ratification at Trust Board: | *January 2012* | Version Number: | 3 |
| Date on Policy Warehouse: | *January 2012* | Team Brief Date: | |
| Circulation Date: | | Date of next review: | January 2014 |

| For completion by ET for *new* policies only: | | | | |
|---|---|---|---|---|
| Additional Costs | | | Budget Code: | Revenue or Non Revenue |
| | (a) Training | £ | | |
| | (b) Implementation | £ | | |
| | (c) Capital | £ | | |
| | (d) Other | £ | | |

# Revisions table

| Revision | Page | Chapter | Date |
|---|---|---|---|
| The security risk assessment should be carried out initially and updated following any change in legislation, or following any security incident, practice, change of area/staff etc. **They should be reviewed at least every two years**. (Emboldened sentence added). | 8 | 5.4 | Sep 2010 |
| Arrangements are in place for ensuring that action is taken as a result of risk assessments | 8 | 5.4 | 4th March 2011 |
| They must undertake risk assessments regarding the physical security of premises and assets in accordance with the Trusts risk assessment guidance using the HSE 5 steps to risk assessment management. | 8 | 5.4 | August 2011 |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

# BARNSLEY HOSPITAL NHS FOUNDATION TRUST

## SECURE ENVIRONMENT POLICY

# I N D E X



**ABBREVIATIONS**

| | |
|---|---|
| Security Management Director | **SMD** |
| Non Executive Director | **NED** |
| Counter Fraud and Security Management Service | **CFSMS** |
| Legal Protection Unit | **LPU** |
| Physical Assault Reporting System | **PARS** |

## 1 .0 STATEMENT OF INTENT

Barnsley Hospital NHS Foundation Trust is committed to protecting the health, safety and welfare of its employees. It strives to provide and keep a safe and secure environment.

The Trust will ensure that all areas are properly secured and have procedures in place to ensure that patients, staff and visitors should be confident they are safe, their personal property is secure and that the Trust's buildings and equipment are protected.

The implementation of this policy requires the total co-operation of all members of management and staff. There will be full consultation with employees' representatives through existing channels of communication.

This policy and any changes made to it will be brought to the attention of all employees who are required to familiarise themselves with it.

## 2.0 INTRODUCTION

This policy has been produced to enable the Trust to positively promote and safeguard security and to introduce and develop a Pro Security Culture within the organisation.

It is the Trust's aim to create a safe and secure working environment for everyone. This includes employees, contractors, visitors and patients.

## 3.0 IMPLEMENTATION

The Trust will properly manage security in the workplace environment by:-

- Appointing and training a Security Management Director, a Resilience & Security Manager and nominating a Non-Executive Director for Security.

- Ensuring that risks associated with physical security of premises and other assets, and the personal safety of patients, staff (including lone workers) and others are identified and managed using the Trust's risk assessment process.

- Ensuring managers and staff understand and carry out their responsibilities for the security of other staff, patients and visitors effectively.

- Developing a culture that provides staff, patients and visitors a safe and secure environment.

- Ensuring that all staff carry out their duties in a manner that ensures the safe keeping of the organisation's property and assets.

- Delivering a staff training programme that encourages and develops a proactive security culture. This will contain practical crime prevention advice and techniques and security awareness will help ensure a safe and secure environment.

- Ensuring that all staff have support if they are involved in a security incident, and are fully de-briefed after the incident.

- Ensuring all staff make the effort to counter the threat of crime; this forms part of the Trust's corporate induction programme as outlined in the training needs analysis on security and maintaining a safe environment.

## 5.0 MANAGEMENT ARRANGEMENTS

### 5.1 Directors Responsibilities

The Chief Operating Officer will be the Security Management Director (SMD) under the Secretary of States' directions 2003.

The responsibilities of the Director are to provide the necessary resources to enable and develop a Pro Security Culture within the organisation.

To ensure that the Care Quality Standards outlined in core standard are met and maintained.

### 5.2 Duties of the Non Clinical Risk Advisor

The Non Clinical Risk Advisor must ensure that: -

- All Security related incidents are reported to the Resilience & Security Manager accredited as the Local Security Management Specialist (LSMS)

- All incidents are properly recorded and the relevant information, trends and actions are placed onto the Trust's incident recording system (IR1).

- All physical incidents are reported to the Counter Fraud Security Management Service (PARS).

### 5.3 Duties of Local Security Management Specialist

To provide professional skills and expertise to tackle security management issues across a generic range of proactive and reactive action. The Resilience & Security Manager will ensure high quality local delivery of this work, within a national legal framework for tackling violence and

security management work, and according to training, standards, advice and guidance provided by NHS Protect.

The overall objective of the Resilience & Security Manager will be 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. This objective will be achieved by working in close partnership with stakeholders within the NHS, the NHS Counter Fraud and Security Management Service (CFSMS) and external organisations such as the police, professional representative bodies and Trade Unions.

**Summary of Duties: -**

- To undertake the duties of a security manager in accordance with Secretary of State Directions to health bodies on measures to tackle violence and general security management measures, and any subsequent advice or guidance issued by NHS Protect

- To undergo and successfully complete proprietary checking and the professional and accredited training in security management provided by NHS Protect, co-operate with any further training provided by NHS Protect and with the NHS Protect programme of quality assurance.

- To ensure that all NHS security management work is carried out within a professional and ethical framework developed and provided by NHS Protect.

- To report to the Trust's Security Management Director (SMD) on security management work locally.

- To lead on day to day work within the Trust to tackle violence against staff and professionals in accordance with the NHS Protect National Framework and Guidance.

- To ensure that appropriate steps are taken to create a pro-security culture within the health body so that staff and patients accept responsibility for this issue and ensure that where security incidents/breaches occur that they are detected and reported.

- To ensure that appropriate security incidents/breaches are publicised appropriately in accordance with guidelines issued by NHS Protect so that a deterrent effect can be created.

- To work towards applying a range of sanctions against those responsible for security incidents/breaches, working with the NHS Protect Legal Protection Unit to ensure appropriate cases are progressed accordingly.

- To undertake a generic Trust wide security audit/risk assessment and provide the Trust Board with an annual report and strategy.

## 5.4 Duties of Managers and Supervisors

Managers and supervisors must ensure that: -

- They and their staff report all security incidents.
- They must debrief staff involved in a security incident.
- All staff shall comply with the Trust's Security Policy.
- They must undertake risk assessments regarding the physical security of premises and assets in accordance with the Trusts risk assessment guidance using the HSE 5 steps to risk assessment management.
- Arrangements are in place for ensuring that action is taken as a result of risk assessments. Actions to include:
    - Profiling the particular hazard/threat
    - Reviewing existing procedures
    - Recording the assessment and actions to be taken
    - Mitigation any risks by:
        - Elimination, reduction or isolation
        - Containment, protection or training.
- They shall carry out a security risk assessment to ensure that the patients, staff and visitors are protected and that all property is secure.
- The security risk assessment should be carried out initially and updated following any change in legislation, or following any security incident, practice, change of area/staff etc. They should be reviewed at least every two years.
- Risk assessment forms can be obtained from the Health and Safety Intranet web page.
- All staff shall attend Mandatory security training
- They uphold good security housekeeping in directorates.
- They consult with staff and their health and safety representatives on all issues relating security.
- Employees adhere to safe systems of work.

## 5.5 Duties of Employees

Employees must ensure that:-

- Must comply with this policy.
- Must report all security incidents.
- Should complete the Trust's IR1incidents report form as soon as they can
- Must comply with all processes and procedures linked to the Trust's security arrangements.
- Must wear their security ID card and ensure it is visible whenever they are on Trust property or business.
- They comply with any instruction and training which is provided in relation to the management of security.

## 5.6 Function of the Trade Union Safety Representatives

- Safety representatives must be meaningfully consulted and involved in risk assessments, safe systems of work involving security related issues and investigations.
- Safety representatives must ensure that they co-operate fully with any security related investigation.

## 5.7 Monitoring Arrangements

This policy and its effectiveness will be monitored annually and this will include:-

1 A comprehensive audit of staff training will be carried out annually; this audit will include a random sample of training objectives and their effective use in the day to day activities.

2 Quarterly reports of all incidents will be reviewed by the Health and Safety Committee, which will include detailed trend analysis, risk assessment and the effectiveness of any follow up action.

3 Risk assessments will be audited as part of any security investigation; all significant and high risk will be entered onto the Trust Risk register.

4 Patient and staff surveys.

5 Annual performance target review, e.g a reduction in incidents, thefts and security breaches.

6 The Resilience & Security Manager will produce an annual report to the Trust Board. This will be used to also monitor the effectiveness of the policy, physical security, Trust's assts and staff training.

7 External verification of the effectiveness of the policy will be undertaken of the policy will be undertaken.

Where the above identifies deficiencies, there will be a requirement to undertake a follow up audit and produce an updated risk assessment.

## 7.0 ASSOCIATED POLICIES AND PROCEDURES

- Violence and Aggression Policy
- Lone Worker Policy
- Access Control Procedures
- Evacuation & Lockdown Policy
- Resilience Policy
- Patients' Property Policy
- Risk assessment Policy and Procedures

## 8.0 POLICY REVIEW

The policy and associated procedure will be reviewed every two years or when there has been a change to legislation

## 9.0 NEXT REVIEW DATE

The policy will be reviewed on or before the 31st December 2013.

## APPENDIX A

## POLICIES AND REFERENCE DOCUMENTS

- Violence and Aggression Policy
- Lone Worker Policy
- Access Control Procedures
- Evacuation & Lockdown Policy
- Resilience Policy
- Patients' Property Policy
- Risk Assessment Policy and Procedures
- Staff Awareness Booklet
- Close Personal Supervision Guidance
- National Counter Terrorist Advice (CONTEST)
- National Resilience Planning Assumptions

## RELEVANT LEGISLATION

- The Health & Safety at Work Act etc 1974
- The Civil Contingencies Act 2004
- The Management of Health & Safety at Work Regulations 1999
- Safety Committees and Safety Representative Regulations 1977
- The Health Safety (Consultation with Employees) Regulations 1996
- The Secretary of States Directions 2003 updated 2009