

Master ID **36**

Version **3**

Document Name **Security Policy**

Type Health and Safety

Date adopted 05 April 2011

Review Date 01 March 2014

Responsibility for Review Local Security Management Specialist

Equality Impact Assessment Performed **Yes**

Approved by

Executive Board

Security Policy

Contents

1. Introduction and Purpose
2. Definitions
3. Accountability and Responsibility
4. Training
5. Personal Safety
6. Premises Security
7. Management of Prisoners attending the Trust
8. Management of Violence and Aggression
9. Lockdown
10. Process for monitoring compliance with and effectiveness of the policy/guidelines/procedure
11. References
12. Consultation
13. Process for review of the document

Appendix A: LSMS Contact Details

Appendix B: Security Management Flow Chart

1. Introduction

NHS Oxfordshire seeks to promote and protect the security of its staff, patients, visitors, contractors, property and information. The Trust seeks to ensure the security and safety of staff and other persons on NHS Oxfordshire premises, or working in the community, on Trust business, at all times.

This policy sets out NHS Oxfordshire's commitment to fulfil its obligations relating to security.

All employees, visitors and contractors have a responsibility to safeguard themselves and their property. Their actions should not put others or the Trust's property at risk. All employees are expected to cooperate with the Trust in the implementation of this policy.

The Trust aims to achieve and maintain compliance with Secretary of State Directions "Violence against staff" (November 2003); and "Security Management Measures" (March 2004). It also aims to take into account guidance issued by the NHS Counter Fraud and Security Management Service (CFSMS), relating to Security Management.

The Trust will seek to:

- Create a pro-security culture;
- Deter and prevent security breaches;

- Detect all breaches that cannot be deterred or prevented;
- Investigate such breaches;
- Rigorously pursue sanctions as appropriate;
- Gain redress in respect of all costs and losses relating to those breaches.

The Trust will encourage staff to report all incidents of assault and security breaches and take appropriate action. As per the Secretary of State Directions incidents must be reported to the Local Security Management Specialist (LSMS). It will seek to identify all costs and losses arising out of security breaches and will consider criminal, civil or disciplinary action as appropriate.

The Trust will take appropriate action to obtain redress in respect of its losses. It will also seek to publicise suitable cases where action is taken against offenders, in respect of security breaches, to deter further such breaches.

The Trust will seek to ensure all necessary support arrangements, such as counselling, are offered in the event of any assault upon staff, and to keep the victim informed about the outcome of any investigation, liaising with the police as necessary. See also the Policy and Guidelines For Dealing With Physical and Non-Physical Assaults Against Staff.

This policy will be monitored, reviewed and updated every two years or as necessary by the Trust's LSMS and the Trust's Security Management Director. Any changes will be subject to Board approval.

The Trust will ensure the safety and security of staff, patients and visitors by having in place an approved documented process for undertaking risk assessments and part of this process will include maintaining an organisational overview of the process and the management of risks.

Risks will be managed by following established crime prevention principles:

- Deterring criminal activity.
- Denying the criminal the opportunity.
- Detecting the crime when it is committed.
- Responding effectively to events.
- Taking corrective action as required to reduce risk.
- Implementing "lock down" procedures in response to risks to staff, patients and visitors.

Reference should be made to other Trust and NHS policies relating to:

- Health & Safety
- Incident Reporting Policy
- SFI's and Standing Orders
- IT Security
- Lone Working Policy
- Disciplinary Policy

2. Definitions

The Trust - NHS Oxfordshire

Policy - The Trusts Security Policy

SSD's - Secretary of states Directions to NHS Bodies 2003 & 2004

Security Breach - An offence against the Trust its staff, patients or visitors that is not covered by the NHS Counter Fraud Service. Examples of security breaches may include: physical or non-physical assaults, theft, criminal damage; unauthorised access to restricted areas or confidential records etc.

CFSMS – Counter Fraud and Security Management Service

LSMS – Local Security Management Specialist

NHSMS – National Health Security Management Service

Lockdown - *Lockdown is the process of controlling the movement and access – both entry and exit – of people (NHS staff, patients and visitors) around a trust site or other specific trust building/area in response to an identified risk, threat or hazard that might impact on the security of patients, staff and assets; or the capacity of that facility to continue to operate. A lockdown is achieved through a combination of physical security measures and the deployment of security personnel.*

Lockdown guidance, February 2009

NB This list is not exhaustive

If you are unsure whether you have witnessed a security breach or need advice relating to this Security policy contact the Trust's Local Security Management Specialist, In the case of a serious incident, the on-call Director must be informed immediately. The LSMS can be contacted as per Appendix A.

3. Accountability and Responsibility

The Chief Executive

Security within the Trust is the ultimate responsibility of the Chief Executive who is responsible for the implementation of this policy throughout the Trust.

The Security Management Director

Security Management Director is the nominated Executive Director with statutory responsibility for overseeing Security Management work. The Security Management Director's responsibilities include, in particular, responsibility for measures to deal with violence against staff.

The Local Security Management Specialist (LSMS)

The Trust's Local Security Management Specialist (LSMS) reports to the Security Management Director. The LSMS' remit is to help deliver an environment, within the Trust, that is both safe and secure. The LSMS is responsible for:

- a) Ensuring that appropriate steps are taken to create a pro-security culture;
- b) Delivering security awareness presentations as required
- c) Undertaking Crime Prevention work - such as Crime Prevention Surveys
- d) Undertaking investigations of security breaches as directed by the Security Management Director in a fair, objective and professional manner;
- e) Undertaking appropriate risk assessments regarding the physical security of premises and assets following a security breach, accident or incident as a minimum or on the request of a manager.
- f) Developing action plans to implement solutions to security risks identified in security risk assessments.
- g) Recommendations brought forward in security audits
- h) Investigations may, with the Security Management Director's agreement, be directed by the Trust's Accountable Officer under the Controlled Drugs Regulations 2006
- i) Ensuring that where a member of staff has been assaulted that appropriate support /counselling has been made available;
- j) Ensuring that the lessons learned from security incidents or breaches are fed into further risk analysis and Crime Prevention work;
- k) Ensuring that security incidents or breaches are actioned and reported as required by the Secretary of State Directions and Counter Fraud and Security Management Service guidance;
- l) Working with the Security Management Director and the NHS Legal Protection Unit to ensure cases are progressed, sanctions are applied, and that redress is sought as appropriate;
- m) Ensuring that security incidents are publicised as appropriate and in accordance with Counter Fraud and Security Management Service guidelines;
- n) The provision of advice and guidance as required to the PCT on security matters;
- o) Producing an annual report and work plan to the Security Management Director and CFSMS on Security Management within the Trust.
- p) Liaising with NHS Security Management Service.

Senior Managers

Senior Managers are responsible for overseeing the implementation of the security policy in their areas of responsibility.

- a) Informing staff of the security policy and making it readily available;
- b) Ensuring that local procedures and protocols are developed as required to maintain the security and safety of all persons, property and information within their areas of responsibility;
- c) Ensuring staff comply with the security policy and follow the procedures and protocols;
- d) Ensuring wherever possible staff are issued with and wear identity cards;
- e) Assessing the training needs of their staff with regard to security issues in particular with respect to Conflict Resolution Training;
- f) Ensuring that staff have access to appropriate information and instructions regarding the security of personal property and PCT premises.

All Staff

All Staff are responsible for:

- a) Ensuring that they read and understand the security policy and make themselves aware of any security procedures particular to their work or the site they work at;
- b) Following the Trust's and their site's specific procedures and protocols regarding the security of people, property and assets, information and premises;
- c) Making full and proper use of equipment provided to maintain security, and reporting any damage, faults or defects;
- d) Informing their managers of any unsafe or potentially unsafe working practices or security problems that may pose risks to them, their colleagues, patients, private or Trust property, or premises;
- e) Informing their managers of any security breaches, security related accidents, incidents or near misses that they are involved in and completing the relevant documentation;
- f) Reporting all incidents involving criminal activity;
- g) While on Trust property or business, wearing Trust identity cards issued to them, and ensuring said cards are visible.

All employees have a responsibility to safeguard themselves and their property. Their actions should not put others or Trust property at risk. Staff must remain vigilant at all times while on Trust property and challenge any persons who are not known to them when safe and appropriate to do so, (staff should not put themselves at risk).

4. Training

The Trust shall provide sufficient training in aspects of "Dealing with Conflict and Aggression" to ensure that all front line staff (Nurses, Porters, Ward Clerks and Receptionists) have been trained in accordance with the training needs analysis and the Secretary of State's Directions that staff shall all be trained by 2008. The course shall be ratified by the CFSMS which shall be certificated, transferable and valid for 3 years.

Should a specific risk be identified and specific training be required this shall be provided in a similar vein. The required training will be organised in liaison with the Learning & Development Department, who will maintain records of training in terms of:

- Criteria for attendance
- The prospectus of training
- Achieved training outcomes
- Any follow up action that is required and by whom

5. Personal Safety

Specific procedures for local needs such as domiciliary visits in respect of lone workers, staff in residential premises, reception staff and non-clinical sites are to be developed and implemented by the individual Directorates.

Staff must follow existing Health and Safety policies and guidelines.

The requirement for security personnel should be assessed by local managers and managed within each area of the Trust. The LSMS shall provide a strategic overview and give assistance upon request.

Departmental managers shall ensure that their members of staff receive and wear ID badges at all times when on Trust property or when undertaking duties associated with the Trust.

Lone Worker – there is a separate policy for Lone Workers

6. Premises Security

The LSMS and Estates and Facilities Directorate in liaison with all stakeholders will identify deficiencies in existing building's internal and external areas that affect security and will programme through the required pathways any remedial works.

In areas of significant risk as identified within the crime reduction surveys to protect staff, assets and property of the Trust physical security devices shall be installed such as: Panic Alarms, Passive Infrared Detectors, Access control, CCTV and other security measures that are at the disposal of the Trust.

Lighting levels in external areas shall be established through the Estates and Facilities Directorate and repairs or future installations will be undertaken through the Estates function of the Directorate.

Bomb Threat/Terrorist threat – is a real live issue in terms of business continuity for any hospital. Processes and procedures for handling such incidents are detailed in the Trusts "Bomb Threat Policy" and "Internal Incident Plan".

The Trust is required to develop a lockdown risk profile for each specific building/area in accordance with CFMS guidance: Locking down the NHS in the Event of Nuclear, Biological and Chemical Contaminants.

7. Management of Prisoners Attending the Trust

This section of policy identifies the care and custody arrangements for prisoners from Her Majesty's Prison Service who require treatment at the Trust, as detailed in the separate policy on the Management of Prisoners.

8. Management of Violence and Aggression

The aim of this policy is to detail the Trust's approach in tackling violence and aggression against NHS staff. This policy has been introduced in the context of the mandatory requirement to report all cases of physical assaults to the NHS SMS. It details the avenues that are available for staff, and the Trust alike, to seek legal redress.

The legal definitions of Physical and Non-Physical assault will be explained, along with detailed guidance on how to deal with incidents involving violence, abuse, threats, intimidation, harassment and other inappropriate behaviours. The policy will

also clearly define the roles of the Security Management Director (SMD) and the Local Security Management Specialist (LSMS) in supporting the Trust staff in dealing with, and tackling, violent and abusive persons.

Please refer to the separate Management of Violence and Aggression Policy.

9. Lock Down

There are a range of incidents (e.g. terrorist attacks; chemical, biological, radiological or nuclear attack) that may require NHS healthcare sites to implement lockdown procedures to safeguard patients, staff, visitors and protect NHS assets.

*Lockdown is the process of controlling the movement and access – both entry and exit – of people (NHS staff, patients and visitors) around a trust site or other specific trust building/area in response to an identified risk, threat or hazard that might impact on the security of patients, staff and assets; or the capacity of that facility to continue to operate. **A lockdown is achieved through a combination of physical security measures and the deployment of security personnel.***

Lockdown guidance, February 2009

A lockdown should be used to ensure the safety and security of all NHS personnel, patients, property and assets in the event of a major incident and by doing so will protect the integrity of the NHS.

Please refer to the separate Lockdown Plan within the Major Incident Plan.

10. Process for monitoring compliance and effectiveness of the policy/guidelines/procedure

Audits of success indicators shall be carried out at a frequency of once every two years or before a policy is renewed or updated. The results shall be provided to the local group that is responsible for approval of the policy, where recommendations and implementation plans will be developed. Ongoing monitoring of the actions shall be overseen by the local group that is responsible for approval of this policy.

Success indicators are a list of the key performance indicators that can be measured and monitored to ensure a policy is being complied with. These success indicators should be audited regularly and feedback reports provided to the local group responsible for approving the policy.

The template below shows an illustration of how success indicators can be presented.

No	Indicator	Factor to be Monitored	Method of Monitoring
1	Roles & Responsibilities	Policy to be disseminated down to staff	Human Resources to measure staff attendance at mandatory training and induction
2	Information for all staff on the management of Security	All staff receive information on induction/mandatory training	Human Resources to measure staff attendance at mandatory training and induction and to be included in all local and mandatory incident training
3	Process for identifying security related matters	Security risks are identified and flagged up using the above flow chart included in the policy	Annual Audit by LSMS
4	Arrangements for the counselling of staff subjected to security related incidents	The frequency and degree of incidents	Incident Reporting system and induction training – Quarterly Governance Report
5	Risk assessment of buildings to be documented in terms of security	To undertake appropriate risk assessment on the physical security of premises and assets	Annual Report and risk assessment portfolio LSMS in conjunction with Facilities and Estates, via SSM's
6	To have a plan to improve security arrangements within available resources	To develop and review an organisation wide action plan following annual risk assessment	Annual review of plan and progress reports through the Health and Safety group

11. References

Trust Policies:

Incident Reporting Policy

Risk Management Strategy

Major Incident Plan

Lone Worker Policy

Management of Violence and Aggression Policy

Lockdown Plan

Physical Assault Reporting Procedure (CFSMS), Department of Health publication
“A Professional Approach to Managing Security in the NHS” 2003

DHSS Report of the Advisory Committee on Violence to staff 1988

Health Services Advisory Committee (HSAC) publication “Violence and Aggression
to staff in Health Services” 1998

Health Service circular 1999/079 “Improvement Targets”

Health Service circular 1999/226 “Campaign to stop violence against staff working in
the NHS: Zero Tolerance

Health Service circular 1999/229 “Working together securing a quality workforce for
the NHS: Managing violence, accidents and sickness absence in the NHS. CFSMS
“Tackling violence against NHS staff” November 2003

CFSMS “A framework for reporting and dealing with non-physical assaults against
NHS staff and professionals” 2004

12. Consultation

For consultation at the Trust’s Health and Safety Committee and initial agreement,
then for the Executive Board to agree and ratify the policy for adoption through out
the Trust.

13. Process for review of the document

The policy coordinator/author will monitor all published policies to ensure that
policies are reviewed in a timely fashion. The Trust policies, procedures and
guidelines shall be reviewed at least 3-yearly, or more often if needed, to ensure
they remain accurate and relevant e.g. to reflect new legislation, new standards and
new evidence of changes in best practice. The Policy Coordinator/author will
maintain a monitoring system and database for this. The review date for all policies
will be included on the document control information include at the front of that
policy.

There are three possible outcomes arising from review of a policy – renewal, rollover
or withdrawal.

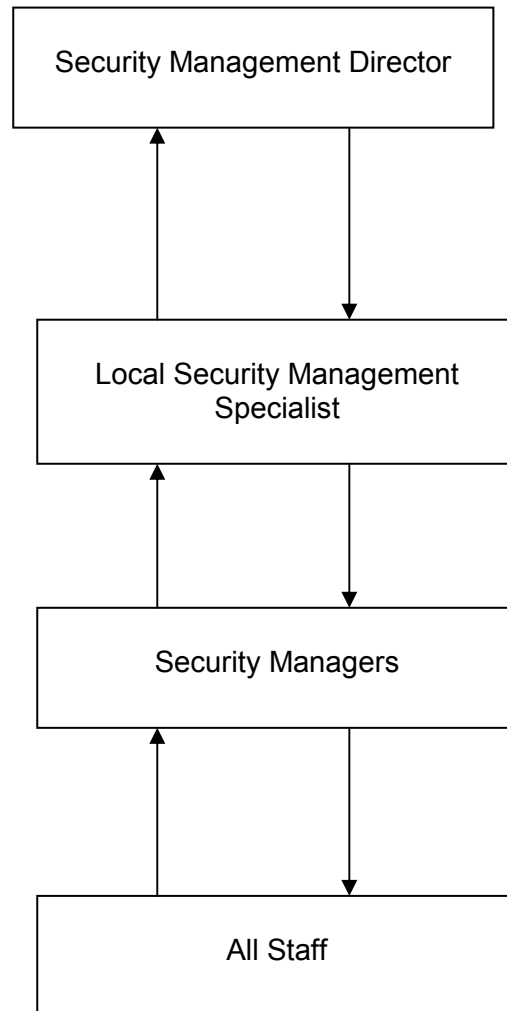
Appendix A

LSMS Contact Details

Name:	Robert Street
Address:	Head Office 135 Greenford Rd, Sudbury Hill, Harrow, Middlesex, HA1 3QN
Mobile Telephone:	07920541665
Email:	Robert.street@parkhill.org.uk
	Robert.street@nhs.net

Appendix B

Security Management Flow Chart



A bottom up and top down process

Security is everyone's business, make it yours!