

# Security Policy

4

## Security Arrangements and Procedures

### **EQUALITY IMPACT**

The Trust strives to ensure equality of opportunity for all both as a major employer and as a provider of health care. This policy has therefore been equality impact assessed by the Risk Management Committee to ensure fairness and consistency for all those covered by it regardless of their individual differences, and the results are shown in Appendix 3.

<b>Version:</b>	<b>4</b>
<b>Authorised by:</b>	<b>Risk Management Committee</b>
<b>Date authorised:</b>	<b>1<sup>st</sup> March 2012</b>
<b>Next review date:</b>	<b>1<sup>st</sup> April 2014</b>
<b>Document author:</b>	<b>Trust Security Manager</b>

## VERSION CONTROL SCHEDULE

Version Number	Issue Date	Revisions from previous issue
1 (final)	October 2005	Original issue. Approved by Trust Executive Group
2	February 2007	Amended following review by Safer Place to Work Group and Risk Management Committee
2.1	February 2008	Amended to include responsibilities for carrying out risk assessments and monitoring arrangements
3	February 2010	Amended on review date and to include generic risk assessments
4	March 2012	The policy was reviewed by the Safer Place to Work group and the Risk Management Committee. The Risk Management Committee requested the policy includes a section on incident reporting. This has now been added to section 8.5 of the policy. The Director of Human Resources is now the designated Security Management Director (previously Director of Planning and Performance)

## TABLE OF CONTENTS

1. INTRODUCTION.....	4
2. OBJECTIVES.....	4
3. SCOPE.....	4
4. DEFINITIONS.....	4
5. DUTIES.....	4
6. POLICY STATEMENT.....	6
7. THE NEED FOR EFFECTIVE SECURITY.....	6
8. SECURITY STRATEGY.....	6
9. POLICY DEVELOPMENT & CONSULTATION.....	9
10. IMPLEMENTATION.....	9
11. MONITORING.....	9
12. REFERENCES.....	10
13. BIBLIOGRAPHY.....	10
14. REVIEW.....	10
APPENDICES.....	11
Appendix 1 SAFER PLACE TO WORK GROUP - TERMS OF REFERENCE.....	11
Appendix 2 RISK ASSESSMENT TOOL.....	13
Appendix 3 EQUALITY IMPACT ASSESSMENT TOOL.....	18

---

## **1. INTRODUCTION**

- 1.1 Tameside Hospital NHS Foundation Trust aims to provide high quality services to the people of Tameside and Glossop through effective and efficient use of resources. This policy and strategy has been developed to support this aim through the provision of a safe and secure environment for patients, visitors and staff. The policy and strategy defines security objectives, sets out arrangements for achieving them and identifies key responsibilities for ensuring the policy and strategy is implemented.
- 1.2 This policy should be read in conjunction with the policies listed in section 8.7

## **2. OBJECTIVES**

- 2.1 The policy aims to manage crime effectively through proactive security measures, effective management systems and the commitment of all managers and staff.
- 2.2 The policy objectives are to ensure:
- The personal safety of patients, staff, and visitors.
  - The protection of property and other assets against fraud, theft, and damage.
  - The provision of a safe environment in which the uninterrupted delivery of quality healthcare can be achieved.

## **3. SCOPE**

- 3.1 This policy applies to all those employed by Tameside Hospital NHS Foundation Trust

## **4. DEFINITIONS**

- 4.1 Security is defined as the state or feeling of being safe and protected.

## **5. DUTIES**

### **5.1 Chief Executive**

The Chief Executive has overall responsibility for ensuring that the Trust meets its statutory obligations and that effective security arrangements are in place and periodically reviewed.

### **5.2 Director of Human Resources**

The Director of Human Resources is the Trust Executive Director with nominated responsibility for security matters as defined in the Secretary of

---

State for Health's Directions to NHS Bodies on Security Management Measures 2004.

### **5.3 Director of Estate and Facilities**

The Director of Estate & Facilities has responsibility for putting in place effective security arrangements and for reviewing these arrangements.

### **5.4 Trust Security Manager**

The Trust Security Manager has line responsibility for developing security management policy and for the operational management of the Trust's security service. The Trust Security Manager discharges the role of Local Security Management Specialist as defined in the Secretary of State for Health's Directions to NHS Bodies on Security Management Measures 2004

### **5.5 All Managers**

Managers are responsible for:

- The development and adaptation of Trust Security procedures to ensure relevance to their specific Directorate/Departmental needs. Risk Assessment & appropriate resource business case bids
- Overall supervision of day to day Security within their Directorate or Department.
- Report crime or suspected crime to the Security Department.
- Ensuring that all staff attend corporate induction.

### **5.6 All Staff**

All members of staff are responsible for ensuring that they comply with Security policies and procedures. It is also essential that any Security incidents involving or observed by staff are reported in accordance with the Trust incident reporting procedure.

### **5.7 Safer place to Work Group**

Site wide risks will be monitored by the Safer Place to Work Group and reported back to the Risk Management Committee on a bi-monthly basis. Site wide risks will be included on the Security Risk Register and will automatically be incorporated into the Facilities Directorate Risk Register and the Trust's Corporate Risk Register where appropriate.

The Facilities risk register incorporating security risks, will be presented to the Risk Management committee twice yearly for review and discussion.

---

## **6. POLICY STATEMENT**

The Trust will (aims to) support the delivery of high quality clinical services, through the provision of a secure environment and by protecting people and property from violence, damage, and theft.

## **7. THE NEED FOR EFFECTIVE SECURITY**

- 7.1 The Trust has a Statutory obligation under the Health and Safety at Work Act 1974 Sections 2 and 3, to manage its activities to minimise the risk of injury or death on Trust premises, and a responsibility to take reasonable steps to minimise the destruction, misuse, or theft of property.
- 7.2 In addition, the Trust has a legal responsibility to provide protection against fire and safety hazards, and to safeguard persons from the unlawful actions of others.
- 7.3 A safe and secure environment complies with legislation and, helps to maintain good relations between the Trust, its staff, and the general public.
- 7.4 The Trust operates on a 24hrs, 7-day week basis and access must be maintained at all times whilst ensuring the security of premises, staff, patients, and visitors.

## **8. SECURITY STRATEGY**

In order to meet the objectives set by its Security Policy, the Trust will implement the following strategy

### **8.1 Deterring Criminal Activity**

The Trust will apply high profile measures such as CCTV, lighting, door access and barrier systems. These will be supported by effective organisational and procedural systems and controls.

### **8.2 Reducing Criminal Opportunity**

The Trust will reduce opportunities for criminals by:

- Incorporating physical protection and crime reduction measures into all designs for new buildings or adaptations to buildings.
- Increasing staff awareness of security issues
- Improving access control systems to buildings, departments and wards

- 
- Improving traffic control systems including the installation of car parking barriers.
  - Improving coverage and effectiveness of CCTV systems
  - The wearing of Identification Badges (ID badges), this enables accurate identification of bona-fide, authorised persons on site.

### **8.3 Effective Response**

The Trust will ensure a quick and effective response to security incidents with workable counter measures to deter illegal activity

### **8.4 Requirement to undertake Risk Assessment**

- Each Ward/Department is required to carry out their own risk assessment for their particular area based on the generic assessment tool. (Appendix 2). Risks must be added to the divisional risk register and managed locally.
- As a result of the local security risk assessment, the Trust Security Manager will identify site-wide risks, and develop appropriate Risk Action Plans where appropriate.
- Funding to address risks identified will be sourced where possible through Capital funding via the Capital Projects Liaison Group, and through PFI works ongoing on the Tameside Hospital site.

### **8.5 Incident Reporting and Crime Pattern Analysis**

8.5.1 Security staff input security incident directly on to the Trust Safeguard incident reporting database. The incident types listed below are then automatically uploaded on the Security Incident Reporting System (SIRS). The information is then collated by NHS Protect to measure the nature and scale of security incidents in the NHS

- Theft of NHS property or equipment
- Theft of Staff or Patient personal property
- Criminal damage to NHS property or equipment
- Criminal damage to staff or patient personal property

8.5.2 Trust staff will be Trust's standard Incident Reporting procedures. The Trust Security Manager will analyse the information provided by these reports, and by other security and crime incident data and will report this analysis to relevant Trust Committees and managers. The Trust will use this analysis to identify improvements in its security measures. encouraged to report all security incidents by using the

## **8.6 A Safer Place to Work Group**

A Trust wide “Safer Place to Work Group” chaired by the Trust Security Manager or designated deputy, and comprising of a wide membership (See Appendix 1), will meet on a bi monthly basis to manage and review the ongoing development and effectiveness of Security Policies and Procedures. Terms of reference for the Safer Place to Work Group can be found in (Appendix 1).

## **8.7 Security Procedures**

Policies and Procedures will be developed and reviewed in a number of areas including:

- Tackling Violence & Aggression Policy
- Management of unintentional aggression policy
- Lone Worker Policy
- Infant abduction policy
- Bomb threats and other emergencies
- Fraud
- Crime Prevention Policy
- CCTV Policy
- Lockdown policy

The Trust Security Manager will coordinate a trust wide Lockdown risk profile as outlined in the Lockdown policy.

Due to limited resources the provisions of the above procedures may need to be introduced as a prioritised rolling programme.

## **8.8 Training**

Trust staff at all levels will attend corporate induction which includes a session on security issues.

## **8.9 Communication Strategy to promote a pro-security culture**

A pro-security culture amongst staff, professionals, patients, visitors, and members of the public is one where the responsibility for security is accepted by all, and the actions of the anti-social minority who breach security not tolerated.

All of the above are fully aware of the standards of conduct expected of them and of the sanctions that may follow unacceptable behaviour.

The methods of communication and dissemination of information to staff of Trust initiatives are:



- Security Awareness Training session to all new Inductees to the Trust, giving an overview of the Security Service, measures implemented by the Trust to Tackle Violence & Aggression and Crime Prevention advice, using examples of previous security concerns within the Trust.
- Safer Place to Work Group – The group helps develop a security conscious culture across the Tameside Hospital site.
- Production of Security related articles for Trust Staff Matters.
- Security Webpage on the TIS website, including details of services, advice and contact details.
- The use of Posters and leaflets to promote Security Awareness
- A list of Security Policies i.e. Tackling Violence & Aggression, Lone Worker Policy, available to all Staff on the TIS Website
- Encourage staff to report all incidents or breaches of security to the Security Control in order to identify problem areas, so that preventative measures can be developed. Staff are also encouraged to report all crimes to the Police.
- Annual Security Awareness Week - A key event in the overall Trust objective to protect Staff, Patients, Visitors, and property at Tameside Hospital. This event will be used to gauge the level of security awareness within the Trust.
- Raise awareness by publicising Breaches of Security to all email users.
- Carry out annual survey of Security Service in order to determine the overall effectiveness of current Security arrangements. Feedback from the survey will be used to assess the overall perceptions of the security provision at TGH, and in addition will form part of the Security Department service plan for the forthcoming year.

## **9. POLICY DEVELOPMENT & CONSULTATION**

- 9.1 This policy was drafted in Consultation with the Associate Director of Facilities, and a Senior Clinical Risk Officer
- 9.2 The draft policy was circulated to the Safer Place to Work Group and Risk Management Committee. Their comments are incorporated into this policy

## **10. IMPLEMENTATION**

- 10.1 The implementation of this Policy will be monitored by the Safer Place To Work Group. The Safer Place To Work Group will provide regular reports to the Risk Management Committee on the Trust's security management arrangements and performance.

## **11. MONITORING**

The Safer Place to Work Group will monitor compliance with this policy. The results of monitoring will be incorporated into an annual monitoring report

---

---

which will be produced by the Trust Security Manager and presented to the Risk Management committee for review and discussion. Where monitoring has identified deficiencies, recommendations and action plans will be developed and changes implemented accordingly. Progress on the action plans will be monitored by the Risk Management Committee.

## **12. REFERENCES**

- 12.1 A Professional Approach to Managing Security in the NHS.  
[http://www.nhsbsa.nhs.uk/SecurityManagement/Documents/sms\\_strategy.pdf](http://www.nhsbsa.nhs.uk/SecurityManagement/Documents/sms_strategy.pdf)

## **13. BIBLIOGRAPHY**

None

## **14. REVIEW**

This policy will be formally reviewed every 2 years, or earlier depending on the results of:

- monitoring,
- changes in legislation,
- recommendations from National bodies, or as a result of
- Incident or accident, complaints or claims data analysis or investigation.

---

## APPENDICES

### Appendix 1

#### SAFER PLACE TO WORK GROUP - TERMS OF REFERENCE

##### 1. Purpose of the Group

To ensure that the Trust provides the best protection for its patients, staff, and property, to allow the Trust to better protect the public's health.

##### 2. Tasks

- 2.1 To advise the Trust Board of its obligations in respect of the security and safety of staff and property, and its performance in managing those obligations.
- 2.2 Monitor compliance with the NHSLA secure environment and violence and aggression standards and provide approved documentation.
- 2.3 To ensure action plans are prepared and delivered to implement new security management guidance and to address any shortcomings in compliance with existing standards.
- 2.4 Prepare communication strategies to support the development of a pro-security culture within the Trust and within Tameside Hospital.
- 2.5 To analyse security incident reports and to ensure action is taken to reduce security risks identified.
- 2.6 To develop a training needs analysis and to ensure that training plans are delivered by relevant departments.
- 2.7 To provide monthly reports to the Risk Management Committee on the Trust's performance in managing security risks.

##### 3. Frequency of Meetings

The Safer Place to Work Group will meet bi-monthly

##### 4. Dissemination of Minutes

The minutes will be distributed to the Risk Management Committee.

##### 5. Membership

###### Core Members:

Security

Emergency/Critical Care

Elective Services

Children's Services

Women's Services  
Risk Management  
Human Resources  
Occupational Health  
Diagnostic & Therapeutic Services  
Balfour Beatty Workforce  
Mitie  
Staff Side

**Invited Non-Essential Attendance:**

Tameside & Glossop  
Pennine Care NHS Foundation Trust  
Greater Manchester Police

**6. Attendance at Committee**

Core members must attend 3 out of 6 meetings per annum.

## Appendix 2

### RISK ASSESSMENT TOOL

Work Area: ..... Date of Assessment:

Assessors Name: ..... Position:

Check the list of potential workplace **HAZARDS/RISKS** and tick which apply to your work area, describe who might be harmed and the existing control measures. Use the risk matrix to estimate the level of **RISK**. Further rows can be added for other hazards that are not listed.

Ref No.	Hazard/Risk: (A hazard has the potential to cause harm)	Applicable to my work area? (Tick)	Who might be harmed Staff, Patients Visitors, Contractors. Also detailing those that might be more at risk, e.g. young, old, disabled, infirm, pregnant employees	Existing Control Measures: (Some examples have been given, check what you currently have in place then record details)	Adequately controlled? If YES please tick. If No please detail what further action is required to control the risk	Consequences of Harm: (C)	Likelihood of Occurrence: (L)	Risk Rating: (C x L)	Date of review ( 1Year max)
	<b>Lone working</b> – <i>Risk of personal injury/ill health/feeling vulnerable</i>		All staff who work alone	Staff aware of 'Lone Working Policy' Lone working tasks are identified and risk assessed, A safe system of working is in place Incident Reporting procedure Safety equipment issued (e.g.					

				mobile phone)					
	<b>Violence or aggression,</b> – <i>Risk of personal injury/ill health</i>		All staff	Conflict Resolution Training Violence & Aggression Policy Management of unintentional Violence & Aggression policy Clear staff handover procedure Medway/Medical Records Alerts Incident Reporting procedure Suitable environment Access to Security assistance Physical security measures					
	<b>Inadequate Door Access Controls:</b>		Buildings, property & staff and patient safety	Electronic Access Control Systems CCTV and intercoms in conjunction with Access Control Systems, to aid identification Local procedures for management of access controls					
	<b>Inadequate Panic Alarm Systems</b>		Staff	Panic alarms linked to ensure a response either within Department/Ward or directly to Security Control Adequate training in response					

				to alarm activation Adequate training in alarm activation					
	<b>Inadequate Physical Security Measures</b> <i>i.e. CCTV, Door Locking Systems, and Barriers.</i>		Buildings, property, staff and patients	CCTV detects and deters criminal activity Locked doors/windows prevent and deter criminal activity Barriers on entry/exits deter vehicle crime Locking up procedures in place					
	<b>Poor lighting at entrance and exits to building/department</b>			Good lighting (plus emergency lighting) fitted on all exit routes.					
	<b>Cash Handling:</b> <i>Patients Money, Petty Cash.</i>		Staff and patients	Patient Property Policy Standing Financial Instructions Secure cash boxes Cash escorts					
	<b>Conflict Resolution:</b> <i>All front line Staff attend.</i>		Staff	Conflict Resolution Training provided – see Trust Training Prospectus					
	<b>IT Security:</b> <i>Loss of IT equipment due to Theft</i>		Staff	All IT equipment security marked and logged with IT Department. Computers fitted with cable locks anchored to a secure fixing					

	<b>Patient Confidentiality:</b>		Staff and patients	Ensure the Trust Policy is observed					
	<b>Handling Pharmacy stock</b> <i>Patient medication etc.</i>		All wards and Departments.	Ensure the Trust Medicines Policy is observed					
	<b>Misuse of prescription pads</b>		Staff and patients	Ensure the Trust Policy is observed Ensure computer is locked when leaving the office. Store prescription forms in locked cupboard in a secure room Never sign blank forms					
	<b>Security of personal property</b> <i>Staff and Patients property.</i>		Staff and patients.	Ensure the Trust Security Policy is observed Ensure lockers are used Staff encouraged to leave valuables at home. Patients valuables must be stored in Night Safe and accurately recorded					
	<b>Unauthorised persons in restricted areas</b> <i>Breach of Patient Confidentiality, Risk of Theft or Physical Attack.</i>			Door access controls in conjunction with staff swipe cards Local procedures implemented and monitored Locked doors to prevent and deter criminal activity					



	<b>All valuable equipment Security marked</b> <i>Risk of Theft.</i>			All equipment security marked and logged on Departmental Asset Register. Ensure equipment is not vulnerable to theft in public areas					
	<b>I.D. Badges.</b>			Photo ID badges to be worn at all times Badges to be visible Challenge any persons without ID Report suspicious behaviour to Security Control					
	<b>Requesting Security Assistance during an Emergency.</b>			Ring Security Control 6688 or Emergency 2222					

Date of Review: .....

By Whom: .....

The risk assessment record must be **REVIEWED** every 12 months as a minimum to ensure that the hazards are still current and the control measures remain effective. They should also be reviewed upon any significant changes to the working environment or working practice and following any serious accident or incident, changes to legislation or guidance, new machinery or processes, new person at increased risk i.e. young, old, disabled, pregnant workers.

The Risk Assessment Record should be held locally.

All significant risk issues must be notified to the appropriate manager.

## Appendix 3

### EQUALITY IMPACT ASSESSMENT TOOL

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