

# **GLOUCESTERSHIRE PARTNERSHIP NHS TRUST**

## **SECURITY POLICY**

Issued: May 2004  
Author: Corporate Services Manager  
Review Date: May 2005

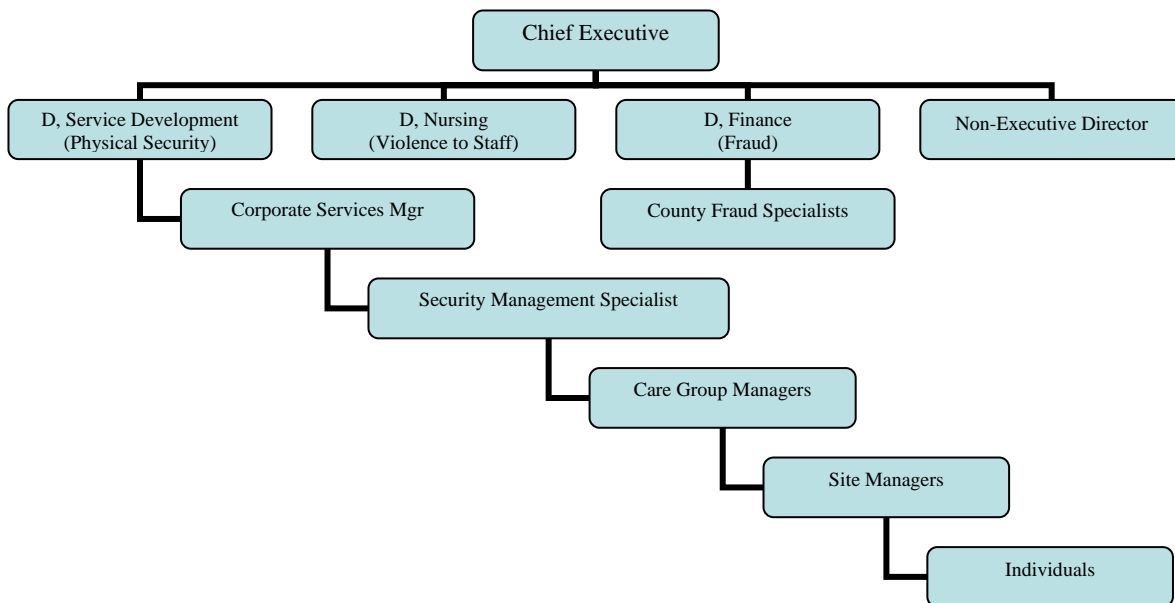
## 1. PURPOSE

- 1.1 This policy is intended to demonstrate the commitment of the Trust Board to supporting managers, employees and patients to enhance both their personal safety and security and that of Trust property and records. It also provides guidance to managers and staff.
- 1.2 This policy is intended to complement, and not replace, the many tried and tested related policies and procedures that have been previously implemented by the Trust.

## 2. RELATED POLICIES AND PROCEDURES

Preventing & Responding to Violence & Aggression  
Standing Financial Instructions  
Information Security Policy  
Identity Badge Procedure  
Fraud Policy  
Working Alone Policy  
CCTV Policy  
Trust Records Policy  
Disciplinary Policy  
Health & Safety Policy  
Fire Policy and procedures  
Guidance for Reporting, Investigating and Preventing Abuse, Exploitation and Neglect in Adults

## 3. ACCOUNTABILITY



## 4. THE BASIC PRINCIPLES OF SECURITY

4.1 Good security should be based on the four following principles:

- 4.1.1 DETER - in security, as in health care, prevention is better than cure. Deterring the criminal will normally be achieved by publicising counter-measures and the degree of success they are having. Effective organisational and procedural systems and controls are an essential element of deterrence.
- 4.1.2 DENY - in the real world, some criminal activity is bound to occur despite efforts to stop it. Good physical protection measures should be taken to deny potential criminals access to patients, staff, goods and assets. By delaying their penetration of physical barriers, the maximum possibility of detection is assured.
- 4.1.3 DETECT - the earlier that criminal acts are detected, the smaller their chances of success. Also, the greater the chances are of preventing the criminal from getting away with it. Raised awareness and technical aids to security are the route to success.
- 4.1.4 RESPOND - without an effective response, other counter-measures may be ineffective.

## 5. RESPONSIBILITIES

5.1 The Chief Executive has devolved Executive Board level responsibility for security:

|                   |                                 |
|-------------------|---------------------------------|
| Physical Security | Director of Service Development |
| Violence to Staff | Director of Nursing             |
| Fraud             | Director of Finance             |

Additionally a non-Executive Director has been designated to promote security management work at Board level.

5.2 Senior Management has a responsibility to ensure that the correct policies and procedures are in place, and that these are regularly reviewed. On a day to day level responsibility for physical security has been delegated to the Corporate Services Manager. The Director of Service Development will prepare an annual security report for the Board.

Essentially, security is about risk management - defining problems and implementing effective solutions. All managers have a responsibility for conducting risk assessments to maintain the safety and security of individuals and property, and for day-to-day monitoring of potential security risks. When conducting security risk assessments the advice of the Trust Fire Officer must be sought to ensure that security measures do not compromise Fire safety. Additional guidance is readily available from the Trust Local Security Management Specialist (LSMS) and local Police Crime Reduction Officers.

### 5.3 Trust Local Security Management Specialist (LSMS)

5.3.1 Once trained and accredited by the NHS Security Management Service, the LSMS will act as the liaison link with the NHS Security Management Service. This role is distinct from counter fraud. It includes protection of patients and staff, Trust property and assets, drugs, prescription forms and hazardous materials.

5.3.2 The LSMS will be required to:-

- Identify problems by analysis of trends and risk assessments
- Work within a clear national strategic framework with a common language of aims, objectives and methodologies
- Create a pro-security culture amongst staff, professionals and the public, engendering a culture where the responsibility for security is accepted by all and the actions of the minority who breach security are not tolerated
- Deter those who may be minded to breach security – using publicity to raise awareness of what the consequences of their intended actions could be, both personally and to the Trust
- Prevent security incidents or breaches from occurring, wherever possible, or minimising the risk of occurrence by learning from operational experience about previous incidents, using technology wisely and sharing best practice
- Detect security incidents or breaches and ensuring these are reported in a simple consistent manner so that trends and risks can be analysed,
- Use this data to properly inform the development of preventative measures or the revision of policies and procedures, both nationally and locally
- Investigate security incidents or breaches in a fair, objective and professional manner, ensuring those responsible for such incidents are held to account and that the causes of such incidents are fully examined and fed into preventive work to minimise the risk of them re-occurring
- Apply a range of sanctions against those responsible for security incidents and breaches, involving a combination of procedural, disciplinary, civil and criminal action as appropriate
- Seek redress through the criminal and civil justice systems against those whose actions lead to loss of Trust resources, through security breaches or incidents, ensuring that those who are the victims of violence within Trust environments are supported to seek appropriate compensation from offenders for loss of earnings or for the effects of injuries sustained
- Develop quality assurance and support mechanisms

5.4 All Staff have a personal responsibility, under Health and Safety regulations to make reasonable efforts to ensure their own safety/security, and that of colleagues. Common sense precautions would include:

- Treating all people with courtesy and respect and avoiding unnecessary conflict
- Keeping personal property safe and out of view
- Informing other staff of possible risks to their personal safety
- Avoiding dimly lit areas at night
- Asking about training
- Reporting all suspicious circumstances, but not placing yourself at risk.
- Dialling '999' if the urgent attendance of the Police is required to deal with any person strongly suspected of committing, being about to commit or having committed a crime. After telephoning the Police it is important that the relevant line manager is made aware of the incident and the action taken.
- Knowing how to get help, particularly if working alone
- Asking for a risk assessment to be completed if you have concerns about safety
- If you feel vulnerable - tell your manager
- If you are physically or verbally assaulted, have personal or Trust property damaged or stolen - report it and ensure the incident is recorded on an IR form.

## **6. REPORTING SECURITY INCIDENTS**

6.1 The Trust will report all relevant incidents to the Police and/or the NHS Security Management Service, and will assist the police in any subsequent investigations. The Trust will make every reasonable endeavour to support employees who have been the victims of security incidents.

6.2 All security incidents, which may include an employees perception of threat, must be reported to the relevant manager for the completion of an IR1 form. The Trust Safety Manager will record all security incidents to inform the LSMS annual Board report and the Trust's risk register. Incidents might include:

physical assault  
car crime  
criminal damage  
theft  
burglary  
robbery  
fraud/deception  
verbal and physical aggression  
other crimes

Incidents involving 'violence' to staff (physical assault, verbal/physical aggression) must always additionally be reported immediately to the LSMS.

## **7. TRUST IDENTIFICATION BADGES**

- 7.1 All contractors must wear Identification Badges. Gloucestershire Partnership NHS Trust staff must adhere to the Identity Badge Policy. This policy can be found within the Partnership Trust Corporate Policy and Procedure folder.

## **8. TRAINING**

- 8.1 The Trust will introduce security and safety lectures.
- 8.2 Security, safety and crime prevention awareness should be included in both Trust and site induction programmes.

## **9. BOMB THREATS**

### **9.1 Preventative Measures.**

All staff should take action, through good housekeeping, to minimise the risk of high explosive bombs being brought into health care premises, particularly in situations of high alert when the police and military authorities suspect the possibility of terrorist activity. Precautionary measures include:

- (1) not allowing rubbish to accumulate on the site
- (2) locking unused cupboards, rooms and buildings
- (3) keeping public areas clear of possible hiding places
- (4) not allowing outside shrubbery to become overgrown
- (5) effective control over the movements and parking of vehicles

### **9.2 Responding to an actual bomb threat**

If, after a bomb threat warning is received directly or via the police, a suspect package cannot be accounted for, the emergency plan should be put into action immediately. If a decision is made to evacuate the building the local fire evacuation procedure should be followed, with the following exceptions:

- (1) leave doors and windows open wherever possible
- (2) leave lights on to assist in any subsequent search
- (3) shut down any plant or machinery where practicable
- (4) the person who found the suspect package, or who received the threat, should be immediately available for interview by the police.

Evacuation should be to a pre-determined assembly point at least 150 metres from the building and out of its line of sight.

Any decision to reoccupy the building or area affected is to be taken by the senior manager present following consultation with emergency services.

Appendix A provides a template which should be readily available to all staff whose telephone can accept 'outside' telephone calls - not only receptionists/telephonists

### 9.3 Reporting

Following every real threat or test of contingency plans, a chronological report of the circumstances and performance of all concerned should be forwarded to the Chief Executive by the site manager.

## 10. **PHYSICAL ACCESS**

10.1 Access points should be restricted to those essential for access. Consideration should be given to converting doors open for convenience only into fire doors. The Trust Fire Office should always be consulted before any access or egress point is closed.

10.2 Individuals on each site, or specific area, should be aware of who has responsibility for checking that windows and doors are properly secured when rooms or areas are vacated. Individuals remain responsible for securing their own work areas.

### 10.3 Key security

All site managers must make appropriate provision for the safe keeping of keys. This provision should include a register to be signed by individuals withdrawing a key from safekeeping. Keys should only be issued to recognised individuals authorised as having access to the locked area.

### 10.4 Alarms

Each site that is unoccupied at night or weekends, or has vulnerable areas which are unoccupied at other times, must conduct a risk assessment to determine whether an alarm should be installed. An alarm is only of real benefit if it is monitored, either by Trust employees or an external security company, to ensure a prompt response. A suitable manager(s) should be available to attend the site if the incident warrants. The Shared Services Procurement team can provide details of companies that can install and monitor alarm systems and provide emergency 'out-of-hours' keyholding response to alarms.

## 11. **ESTATES**

11.1 Any Business Case or bid for capital that involves new builds or property renovations is always to include confirmation that the Trust LSMS has been consulted on the design and that the design has considered and adopted all necessary security measures. This consideration should always include clinical input where appropriate.

11.2 Estates shared services will ensure all Trust premises are provided with suitable door and window locks to give a good level of security. All digital 'key pad' locks should have access numbers changed at least every six months, or when there is any suspicion that the numbers have been compromised.

- 11.3 The Trust LSMS will carry out security surveys of buildings and will seek advice, as necessary from the Police Crime Prevention Department and the Trust Fire Safety Adviser.
- 11.4 Managers, in consultation with Trust LSMS should regularly review the external security of sites – particularly with regard to staff safety. Areas to be considered should include: adequate lighting of paths, car parks and entry/exit areas, removal of shrubbery and introduction of CCTV.

## **12. MONITORING OF POLICY**

- 12.1 This policy will be monitored by the completion of a 6-monthly report by Care Group Managers to the Director of Service Development and by the annual report made to the Trust Board. Care Group Managers will be asked to report on the subject headings contained in this policy, and to advise on any specific areas of concern.
- 12.2 Further monitoring of the content of the policy will form part of the Trust's annual submissions under Controls Assurance audit requirements.
- 12.3 This policy will be reviewed bi-annually and may be updated in the interim as necessary.

## **13. TRUST SECURITY MANAGEMENT SPECIALIST**

- 13.1 The Trust is required to nominate a Security Management Specialist for training and accreditation by 31<sup>st</sup> March 2004. The Security Management Specialist will provide a security service for management and staff and will provide advice and guidance on all security issues. In association with Director of Finance and the Fraud Officers s/he will investigate losses and will liaise with the Police.
- 13.2 The security management specialist will also monitor all reported crime (via copies of IR1's from Trust Safety Manager and will submit an annual report to the Corporate Services Manager for inclusion in the report to the Trust Board.

## **14. LIKELY RESOURCE IMPLICATIONS**

- 14.1 Gloucestershire Constabulary Crime Prevention Officers may provide security lectures/briefings for staff at no charge.
- 14.2 The Home Office will provide appropriate literature and publicity material at no cost.
- 14.3 Recruitment of a Local Security Management Specialist

**Actions to be taken on receipt  
of a Bomb Threat**

- Switch on Tape Recorder (if connected)
- Tell the caller which town/district you are answering from
- **Record the exact wording of the threat**

.....  
.....  
.....  
.....

- **Ask these questions**

1. Where is the bomb right now? .....
2. When is going to explode? .....
3. What does it look like? .....
4. What kind of bomb is it? .....
5. What will make it explode? .....
6. Did you place the bomb? .....
7. Why? .....
8. What is your name? .....
9. What is your address? .....
10. What is your telephone number? .....

- Record time call completed

.....

- **Keep telephone line open (even though call has disengaged)**

- Where automatic number reveal equipment is available record number shown

.....

- **Inform** (Trust on-site manager and, out of hours, senior on call manager)

- **Contact the police by using the emergency (999) telephone number**

Time police informed .....

**COMPLETE THE FOLLOWING ONCE CALLER HAS HUNG UP AND POLICE/MANAGER HAVE BEEN INFORMED**

Time & date of call .....

Length of call .....

Your extension number .....

**About the Caller**

Sex of caller? Male  Female

Nationality? ..... Age? .....

**Threat Language**

Well spoken  Irrational  Taped

Foul  Incoherent

Message read by threatmaker

**Caller's Voice**

Calm  Crying  Clearing Throat  Angry

Nasal  Slurred  Excited  Stutter

Disguised  Slow  Lisp  Accent

Rapid  Deep  Familiar  Laughter

Hoarse

If the voice sounded familiar, who did it sound like? .....

\*What accent? .....

**Background Sounds**

Street noises  House noises  Animal Noises

Crockery  Motor  Clear

Voices  Static  PA system

Booth  Music  Factory Machinery

Office Machinery

Other (specify) .....

**Remarks**

.....  
.....  
.....  
.....  
.....  
.....

Signature.....

Date.....

Print name.....