SECURITY OF PREMISES AND ASSETS

NGH-PO-116

Ratified By:	PDG Group
Date Ratified:	June 2014
Version No:	6
Supercedes Document No:	5.9
Previous versions ratified by (group & date):	Procedural Documents Group
Date(s) Reviewed:	June 2014
Next Review Date:	June 2017
Responsibility for Review:	Deputy Hotel Services Manager
Contributors:	Deputy Hotel Services Manager

POLICY

CONTENTS

POLICY

Version Control Summary

Version	Date	Author	Status	Comment
6	April 2014	Andrew Watkins	Deputy Hotel Services Manager	Ratified

SUMMARY

This policy provides information on internal and external security of the site, along with risk assessments

Contact Numbers	
security in an emergency	**2222**
The Trust's Local Security Management Specialist LSMS for any matters on security including sensitive and confidential issues.	5726 or bleep 4333
The Portering and Security Manager, extension is available to provide assistance or advice on any security related matter.	5473 or bleep 4400
Security officers can be contacted at any time, 24 hours a day	5740 or bleep 1305.
Car Park Security	bleep 1306 (Monday to Friday 08:30 – 22.00) bleep 1305 (out of hours)

1. INTRODUCTION

Hospitals and Healthcare premises are private property but open to the general public with 24-hour open access.

Losses, whether from crime or damage, are paid for from Trust resources. This affects the Trust's overall performance and, more directly, reduces the funding available for direct patient care.

Crime is not always committed by professionals, but often by those exploiting easy opportunities. Individuals steal when the opportunities arise i.e. when valuables and goods are left unprotected within wards and departments

In December 2003 the Secretary of State launched the Security Management Strategy " A Professional Approach to the Management of Security in the NHS" This can be downloaded at http://www.nhsbsa.nhs.uk/ then click on the NHS Protect link. The document outlines how the NHS will provide the best possible protection for its patients, staff, professionals and property. NHS Protect will carry this forward. The main objective of this strategy is the delivery of an environment for those who work in or use the NHS that is properly secure so that the highest standards of clinical care can be made available to patients.

The Secretary of State has clearly outlined how this new approach will affect management of Security in the NHS. These Directions will create a structure to implement the strategy and define the roles and responsibilities of Trusts and the SMS. NHS Protect

This policy represents the key for management and staff to actively take control of their environment, and remove opportunity in order to prevent crime. It is the obligation of every member of staff to support the Trust Policy and NHS Protect directions by contributing towards creating a safe and secure environment for all those who use the Trust services.

2. PURPOSE

The purpose of the Security Policy is to ensure the physical security of premises and assets that protects patients, staff, and visitors of the Trust by establishing a secure climate that deters criminal activity.

The key objectives are: -

- The protection of confidentiality. (The Information Security Policy and Procedure - Corporate Policy 011 and Data Protection Policy – sets out Trust compliance requirements and guidelines for handling information in accordance with the Data Protection Act and the NHS Confidentiality Code of Practice)
- The protection of property against loss, fraud, malicious acts, damage and trespass.
- The detection and reporting to management of criminal offences, which are in breach of the Security Policy.
- To meet the Secretary of States Directions of 2003 in providing a safe and secure environment in line with the NHS Protect security management manual.

3. SCOPE

This policy applies to all areas of the Trust including any areas that are offsite and all individuals employed by the Trust including contractors, voluntary workers, students, locum and agency staff.

4. COMPLIANCE STATEMENTS

Equality & Diversity

This policy has been designed to support the Trust's effort to promote Equality and Human Rights in the work place and has been assessed for any adverse impact using the Trust's Equality Impact assessment tool as required by the Trust's Equality and Human Rights Strategy. It is considered to be compliant with equality legislation and to uphold the implementation of Equality and Human Rights in practice

.

NHS Constitution

The contents of this document incorporates the NHS Constitution and sets out the rights, to which, where applicable, patients, public and staff are entitled, and pledges which the NHS is committed to achieve, together with the responsibilities which, where applicable, public, patients and staff owe to one another. The foundation of this document is based on the Principals and Values of the NHS along with the Vision and Values of Northampton General Hospital NHS Trust.

5. DEFINITIONS

Theft	A person is guilty of theft if dishonest appropriates property belonging to another with the intention of permanently depriving the other of it. (Theft Act 1968)
Criminal Damage	destruction or damage to any property without lawful excuse, destroys or damages, any property belonging to another intending to destroy or damage any such property or being reckless as to whether any such property would be destroyed or damaged shall be guilty of an offence. (Destroying or Damaging Property Section 1 (1) – Criminal Damage Act 1971)
Physical Assaults	The intentional application of force against the person of another without lawful justification, resulting in physical injury or personal discomfort. (NHS Protect Management Manual - First edition March 2005)
Non-Physical Assaults	The use of inappropriate words or behaviour causing distress and/or constituting harassment. (NHS Protect Management Manual – First edition March 2005)
Harassment	Is defined, for the purpose of this policy, as the impact, not the intention of the behaviour and may take many forms, being directed at an individual or a group from members of the public. This is: Any action, behaviour comment or physical contact, which can reasonably be deemed to be offensive to the person involved and which causes that person to feel threatened, humiliated or embarrassed. (NHS Protect Management Manual – First edition March 2005)
NHS Protect	Leads on work to identify and tackle crime across the Health Service
LSMS	Local Security Management Specialist
Assets	Is a generic term which can mean any type of fixed and unfixed equipment such as furniture, medical equipment, IT equipment, vehicles and any such item procured through and for the Trust.
Premises	Grounds and buildings belonging to and or managed by NGH NHS Trust
Business Visitors	Those who have been invited to attend meetings, presentations and training by a member of NGH staff

6. ROLES & RESPONSIBILITIES

ROLE	RESPONSIBILITY
Chief Executive and the Trust Board	Are responsible for ensuring there is a policy in place.
Security Management Director (SMD)	The Director of Facilities and Capital Development will assume this role and be responsible for the strategic development and the operational provision of Security Services. The Director of Facilities will report the status and progress of Security activities within the Trust to the Chief Executive and as necessary to both IHGC and Trust Boards.
Local Security Management Specialist (LSMS)	The Trust's Deputy Hotel Services Manager assumes this role. This role has been developed in line with the NHS Protect. The LSMS will report directly to the SMD. This role will include: a) To support on day-to-day work within the Trust to tackle violence against staff, visitors and patients in accordance with the NHS Protect national framework and guidance. b) To ensure that appropriate steps are taken to create a pro-security culture within the Trust so that staff and patients accept responsibility for the issue and ensure that where security incidents/breaches occur that they are detected and reported. c) To investigate security incidents or breaches. (The Data Protection & Confidentiality Manager is responsible for investigating Data Protection Act and confidentiality breaches). d) To work towards applying a range of sanctions against those responsible for security incidents or breaches. e) Review risk assessments sent from managers and heads of department with Deputy Director of Facilities to evaluate if there is a physical security implication. Those with a risk rating of moderate or above are to be discussed with the SMD by the LSMS to determine if any action is required to mitigate risk and how soon this should occur.

Portering and Security Manager	Will manage all security officers ensuring there is 24/7 cover. Will chair Hospital Watch on a quarterly basis and provide minutes of meetings.
Line Manager	Each department and ward shares in the responsibility for ensuring that staff within their environment adheres to the Policy. It is essential that managers allow staff the time to read through this policy and be given the opportunity to discuss the policy either with their Line manager or any member of the Security Team. Management must consider the implications for Security when drafting new procedures, purchasing equipment and designing new or re-designing operational space they should seek advise from the trusts LSMS Managers must ensure that all staff working within their areas has official identification, which is available at all times whilst on duty. Managers are responsible for carrying out annual Security Risk Assessments of their areas or sooner if an incident has taken place or if it is felt there is a need to improve security of the area. Guidance can be found in Appendix 2 assessment tool. Copies should be retained by the department and a copy forwarded to the Trusts LSMS. Where security risks have been identified these should be reported by the manager to the Directorate Health and Safety .Group. This Group will then escalate concerns security risks that cannot be mitigated to the Trust Health and Safety Committee.
All Trust Employees	Have a responsibility to: • Support the Trust to achieve its Vision • Act at all times in accordance with the Trust values • Follow duties and expectations of staff as detailed in the NHS Constitution – Staff Responsibilities Security is everybody's business. Proactive staff, who understand the potential risks are the best deterrent to crime. It is the duty of all staff to be vigilant, remove temptation from criminals and promptly report, to the Security Department, LSMS or the Police, any incidents or suspicious circumstances.
Health and Safety (Trust)	Responsible for having a Trust wide overview of security risks that cannot be mitigated by a directorate. This Committee will determine action required and the LSMS will report to Trust Board annually.

7. SUBSTANTIVE CONTENT

7.1. Annual Security Review

The Trust is committed to ensuring security remains a high profile subject and as such the Trust's LSMS will produce an annual security report to the Trust Board agreed by the Trusts SMD to reflect on progress, incident reporting data analysis, achievements for the financial year highlighting the forward direction of security including prioritised security requirements and initiatives. The Security Report is reviewed and actioned on a year on year basis.

7.2. Security risk assessments

Each department head are required to carry out an annual security risk assessment and submit to the Directorate health and Safety committee. When a security risk is identified this should be discussed at Directorates Health and Safety meetings and where it is agreed it needs to be escalated this should be submitted to the Trusts Health and Safety group. These should be entered onto the Directorates and Trusts Risk Register (if 15 or above)

The LSMS will review these with the Deputy Director of Facilities and submit security risk concerns to the SMD. The SMD will agree security organisational overview through the Trust Board.

7.3. Incident Reporting Procedures

The list below shows what should be done when an incident takes place and is reported.

a) Complete an incident report on the Datix system and report incident to a manager or supervisor.

b) The Security Department will investigate incidents when informed. Where a crime is established, the police will be consulted and a crime number allocated. The Information Governance Manager is responsible for investigating Data Protection Act and confidentiality breaches.

c) From its records, the Security Department will collate statistical information in order to identify specific problems and target action.

d) Where a crime is committed against an individual, within the Trust, it is their responsibility to report it to the Security Department

The LSMS and Portering and Security Manager are available to offer advice, support and investigate incidents

7.4. Staff Identification

It is a Trust requirement for all staff to wear official identification whilst on duty. All permanent staff and temporary/bank staff working more than a month must have photographic I.D. To arrange for photo I.D. contact Main Reception Cliftonville on 5475 Monday-Friday 09.00-17.00. All staff should wear a name badge which identifies name and job role.

Temporary staff employed for less than a month, bank/agency staff and locums must collect a temporary staff pass from Main Reception Cliftonville between 09.00-17.00 Monday - Friday. A pass will only be issued on confirmation of post covered. This may be through confirmation letter from Human Resources or the department the staff is working for, this will need to be shown to the receptionist or if a senior staff member accompanies the temporary staff from the department who can confirm their identity.

OR

The person must have visible ID, which indicates they are employed by a registered/approved agency that the Trust has contracted to provide a service. The Security Dept must be informed of these providers and types of ID.

- Identification sets staff apart from the public.
- Bogus employees are a reality. It could happen at this Trust and staff must be prepared.
- Security passes and identification badges must be worn, and visible, by every member of the Trust. Managers must ensure that all their staff are clearly identified.
- Access by staff cannot be justified without sight of identification.
- Report loss of ID to the Travel Office or Security Department as soon, as is practical. When the I.D. has access to secure doors and car parks must be reported immediately to the Travel Office (5966) or the Security Department (5780). The card will be de-programmed from the system.
- Loss or damage to ID card will incur a replacement cost.
- Security will randomly stop staff and ask to check their I.D. Staff not carrying correct I.D. will be advised accordingly.

It is the Manager's responsibility, upon termination of employment, to ensure that ID cards are returned to Main Reception Cliftonville so that they can be deactivated.

7.5. Visitor Identification

It is the responsibility of Departmental / Ward Manager's to ensure any business visitors or representatives to their wards or departments are escorted or are issued with temporary ID. Non-Trust staff should not be allowed into secure areas unless accompanied by a staff member.

Visitor passes can be obtained from Main Reception Cliftonville between 09.00-17.00 Monday-Friday. A visitor pass will only be issued to a visitor if accompanied by a member of staff from the area they are visiting. Visitor passes can be collected by dept/ward in advance of a visit by contacting Main Reception on 5475.

Some departments have their own booking in procedures. Where this takes place Heads of Departments must ensure their systems are robust and audited regularly, i.e. are all visitors/staff where applicable being booked in, can they be accounted for within an area and are passes returned and visitors booked out

Contractors who are carrying out works on behalf of the Estates Services must first report to the Estates Reception and collect a visitor's pass before commencing their duties. If any member of staff is unsure about a contractor visiting their area to carry out works then they should contact the estates Services General Office on 5444 or 4860 for verification or in an emergency 2222.

Non Estates contractors, it is the responsibility of the Department requiring the contract work to be undertaken to ensure they are satisfied that they hold relevant insurance details, risk assessments and method statements to allow the work to proceed at no risk to the Trust.

7.6. External Security

One of the primary aims of the Security Policy is to ensure the Trust, its wards and departments are as secure as possible. However, the 24-hour open access nature of the Trust means that, in order to achieve this aim, investment has to be in door access control systems and intruder alarms as well as conventional mortice and Yale type locks. These systems are supported by a physical Security Officer presence, through regular patrols.

Departments are responsible for securing their departmental area. The last person leaving should ensure all areas are secured.. Where security identify insecure areas they will secure and a Security Incident Report completed, this will be forwarded onto the relevant departmental head. It is expected that the departmental head will remind staff of their responsibilities in securing their work area.

Closed Circuit Television (CCTV) is seen by the Trust to represent an essential tool in monitoring on site security and is managed in accordance with the Information Commissioner's CCTV Code of Practice. There are 66 CCTV cameras directly linked back to the CCTV control room operating and recording 24 hours a day covering car parks, entrances and internal areas. There are further cameras that are linked directly within departments monitoring access doors for their areas.

It should be remembered that any alarm or locking system, however sophisticated, becomes useless when a window or door is left open.

Most thieves are not hardened professionals, but simply amateurs waiting for an opportunity. Digital door entry systems are useless if the combination code is freely available.

7.7. Car Park Security

Car crime is a major problem nationwide, CCTV supports the security department in its fight against car crime. Staff should report any suspicious activity within the Hospital car parks. CCTV will continue to be developed on the Trusts premises having proven its worth as a deterrent in reducing overall crime

All staff vehicles parked on site must display correct car parking I.D. permit issued by the Travel Office. To obtain car-parking permit the relevant car parking form must be fully completed and signed by the departmental authorised signature holder. The form must be taken to the Travel Office to be processed. Failure to display the correct permit may result in the vehicle receiving an enforcement notice (parking ticket)

7.8. Internal Security

It is the responsibility of all staff to ensure security is maintained. Vigilance and careful staff are the key to successfully reducing crime.

The following security measures are in place across the Trust:

Door locks, ID cards, digital locks, window locks, lockers, CCTV, recording equipment, Security Officer patrols, ID marking of Trust property.

It is essential that these devices are properly and efficiently used. Potential thieves are quick to spot areas of weakness. Lax procedures such as leaving keys freely available, door codes widely made available, alarms not checked, lockers left insecure are sure to be exploited.

Managers must maintain an effective access control system when allowing staff or visitors into secure areas.

7.9. Cash Handling

Standing Financial Instructions (S.F.I`s paragraph 6): **(Income, Fees, Charges and Security of Cash, Cheques and other Negotiable Instruments)** must be adhered to when dealing with cash and cheques. For further advice the Director of Finance should be contacted. Advice should be sought from the Security Department concerning movements of cash etc around the Trust.

Cash is particularly attractive to thieves. Notes and coins are hard to identify, easy to conceal and easy to dispose of. Protecting cash demands continual vigilance from staff.

Borrowing or lending of money from tills, petty cash etc. is totally unacceptable and infringements of this rule constitute gross misconduct and could result in dismissal from the Trust. Each departmental Manager is responsible for the accuracy of all collected cash and should carry out regular audits to ensure that procedures are strictly adhered to.

7.10. Hospital Watch

The Hospital Watch Group meet quarterly attended by a nominated staff member from Care Groups and departments and chaired by the Portering and Security Manager Also in attendance is the Trusts LSMS and representation from the Police.

The purpose of this group is for the Portering and Security Manager to report on crime, violence and incidents that have occurred across the Trust since the previous meeting. Planned or proposed initiatives are collectively discussed.

Representatives are expected to report back to staff, discussions that have taken place and make them aware of security incidents and any initiatives in place, proposed or planned. Staff should also be able to approach their representative who can convey on their behalf information and ideas to the group.

It is important that representatives attend these meetings as it helps promote and identify security issues across the Trust.

7.11. Violence, Aggression and Harassment Against Staff

The security department endeavour to protect staff against violence, aggression and harassing situations this policy should be read in conjunction the ***PROTECTING STAFF AGAINST VIOLENCE, AGGRESSION AND HARASSING SITUATIONS FROM PATIENTS AND MEMBERS OF THE PUBLIC (Corporate Policy No NGH-PO-46).*** It is important that staff read this policy as this explains in detail what actions the Trust can and will take against aggressors and harassers to staff.

7.12. Theft Carried Out By Employees

The National Health Service in common with most organisations suffers from crime by its staff ranging from petty pilfering to more serious crimes- the cost of which runs into millions of pounds. The Trust is committed to eliminating the drain on resources which crime causes, whether from the public or its own employees. Theft is considered as Gross Misconduct within the Trusts Disciplinary Policy (NGH-PO-028), which may lead to dismissal and criminal prosecution through either the police or private prosecution through the Trust and/or the NHS Protect.

Staff maybe asked with their permission to be searched or have their bags, locker, desk or any other type of storage facility searched by security in the presence of a manager to identify if a crime may have been committed. It should be noted that to be searched is voluntary and only the police have the legal powers to search without having to ask for permission. If a member of staff declines to be searched, have their bags, locker desk or any other type of storage facility searched then this will be seen as a possible disciplinary matter and further investigated and/or security will call the police and ask them to attend and carry out a search.

7.13. Data Security, Protection and Confidentiality

The Data Protection Act- Principle Seven – requires the Trust to adopt appropriate technical and authorised measures to protect against unauthorised or unlawful processing, accidental loss or destruction or damage to information relating to identifiable living individuals held in paper or electronic format.

Any breach of confidentiality, whether of patient or staff data or Trust business, may result in disciplinary action in accordance with the Trust's Information Security Policy (NGH-PO_011) and Data Protection Policy(NGH-PO-334). These Policies are available on the Intranet and staff should acquaint themselves with the content.

7.14. Lone Working

Some staff by the necessity and nature of their employment may have to work in situations within the Trusts property i.e. Departments, Offices in or out of normal working hours alone.

Whenever possible staff should utilise the official Department /Offices opening hours where other staff are likely to be present. When this is not feasible and arrangements or situations require staff to work alone in or out of hours certain steps must be taken to ensure their personal safety for example:

- Main doors should be locked or if fitted with a key/swipe pad this should be used.
- Do not open doors to anyone unless identity has been established.
- Seek advice from Security, Risk Management or/and Trusts LSMS.
- Risk assessments should be undertaken within the work place and include the type of work undertaken.

All staff have a responsibility to advise colleagues within their Departments / Offices if they are the last member of staff within the Area.

It is the responsibility of individual staff who work alone to assess the risks involved and take appropriate steps to minimise compromising their safety. It is the responsibility of the last member of staff to leave the Department/office to ensure that Safety checks and locking up procedures are carried out a local level and within Departmental guidelines.

Related Guidance

.

- Lone Working Policy NGH/PO/236
- NHS Protect, Not Alone – A Guide for the Better Protection of Lone Workers in the NHS (2009)

7.15. Recruitment Guidelines

Northampton General Hospital are committed to ensuring that current recruitment and selection tional guidance is adhered to particularly in relation to criminal records checks. For current policy please refer to the Recruitment and selection and retention policy. (NGH-PO-033)

7.16. Lockdown Risk Profile

In February 2009, the NHS SMS published guidance for Trusts on planning and completing a physical lockdown of the site (SMS 2009) The Trust currently has a Lockdown Plan which will instruct staff on how to coordinate a partial or full lockdown based on the nature of the event. The Trusts Security Department on a daily basis locks down the hospital during the evening out of hours and re-opens from 5.00am. (see APPENDIX 3) This approach would currently be adopted if the Trust had to full lock down or initiate a partial lockdown

Related Guidance

- NHS Protect Lockdown Guidance (Updated February 2009)
- NHS Emergency Planning Guidance 2009 (Department of Health)

7.17. Key Messages

- Keep valuables locked away, if you have a locker use it and lock it.
- Keep your cash/credit cards with you or as a minimum locked away.
- Do not carry large amounts of cash.
- Ensure that windows and doors are locked when buildings are vacated.
- Report all incidents to Security and your departmental head.
- Ensure your safety when working alone, secure doors, inform others they are the last member of staff within the department / area.
- Ensure your safety when working within the community.
- Set alarms before leaving department.
- Equipment should be securely stored and ID asset marked if applicable to item.
- Door/Alarm codes should only be issued to authorised users

8. IMPLEMENTATION & TRAINING

Implementation

This policy should be implemented and disseminated immediately and be a live working document. It will be published on the Trusts intranet site.

Training

The Learning and Development department organise Conflict Resolution courses and breakaway training courses through the year. Dates are available from the training department (5751).

Advise on appropriate training needs can be discussed with the Trusts LSMS, Portering and Security Manager or the Learning and Development Department.

9. MONITORING & REVIEW

Minimum policy requirement to be monitored	Process for monitoring	Responsible individual/ group/ committee	Frequency of monitoring	Responsible individual/ group/ committee for review of results	Responsible individual/ group/ committee for development of action plan	Responsible individual/ group/ committee for monitoring of action plan
Each department undertakes annual risk assessment	Complete/review security assessment form.	Directorate H&S/Governance Group Mins Directorate risk register	Agenda item as per meeting dates	Directorate H&S/Governance Group	Chair of Directorate H&S/Governance Group	CQEG
There is an organisational overview of risks associated with security of premises through the SMD and LSMS for future security measures development	Escalation to H&S committee of unmitigated security risks from directorates (H&S Mins) Trust Board annual security report	Deputy Director Facilities and LSMS LSMS and SMD	BI-Yearly	Deputy Director Facilities and LSMS	Deputy Director Facilities and LSMS	SMD

10. REFERENCES & ASSOCIATED DOCUMENTATION

Department of Health (2004) *Secretary of State directions on NHS Security Management Measures* [online] London. DH. Available from: http://www.nhsbsa.nhs.uk/SecurityManagement/Documents/lsms_nomination.pdf

NHS Protect (2012) *Guidance on the management and security of NHS assets* [online] NHS Protect. Available from: http://www.nhsbsa.nhs.uk/Documents/SecurityManagement/Property_and_assets.pdf

NHS Security Management Service (2009) *Tackling violence against staff: explanatory notes for reporting procedures introduced by Secretary of State Directions in November 2003 (updated June 2009)* [online] London. NHSBSA. Available from: http://www.nhsbsa.nhs.uk/SecurityManagement/Documents/SecurityManagement/Tackling_violence_against_staff_2009.pdf

NHS Security Management Service (2004) *Conflict Resolution Training: implementing the national syllabus* [online] London.NHS Security Management Service. Available from: http://www.nhsbsa.nhs.uk/SecurityManagement/Documents/crt_implementing_syllabus.pdf

NHS Security Management Service (2004) *Non Physical Assault Explanatory Notes: A framework for reporting and dealing with non-physical assaults against NHS staff and professionals.*[online] London. NHS Security Management Service. Available from: http://www.nhsbsa.nhs.uk/SecurityManagement/Documents/non_physical_assault_notes.pdf

Data Protection Act 1998 (c.29) [online] London. HMSO. Available from: http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_1

Department of Health (2003) *NHS Confidentiality Code of Practice* [online] London. DH. Available from*:* https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200146/Confidentiality_-_NHS_Code_of_Practice.pdf [Accessed 14th December 2010]

Rehabilitation of Offenders Act 1974 (exceptions) order 1975 [online] London. HMSO. Available from: http://hansard.millbanksystems.com/lords/1975/jun/19/rehabilitation-of-offenders-act-1974 [Accessed 1st May 2014]

Department of Health (2013). *NHS Constitution: the NHS belongs to us all.* [online]. London. Department of Health. Available from

Department of Health (2013). *NHS Constitution: the NHS belongs to us all.* [online]. London. Department of Health. Available from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/170656/NHS_Constitution.pdf

NHS Counter Fraud and Security Management Service (2003) *A professional approach to managing security in the NHS* [online] London. DH. Available from: http://www.nhsbsa.nhs.uk/SecurityManagement/Documents/sms_strategy.pdf

Northampton General Hospital NHS Trust (2013) *Data protection and confidentiality*. NGH-PO-334. Northampton. NGHT.

Northampton General Hospital NHS Trust (2014) *Information security*. NGH-PO-011. Northampton. NGHT.

Theft Act 1968 (c.60) [online] London. HMSO. Available from: http://www.legislation.gov.uk/ukpga/1968/60/contents

Criminal Damage Act 1971 (c.48) [online] London. HMSO. Available from: http://www.legislation.gov.uk/ukpga/1971/48/contents

Northampton General Hospital NHS Trust (2011) *Protecting staff against violence, aggression and harassing situations from patients and members of the public.* NGH-PO-046.

Northampton General Hospital NHS Trust (2013) *Lone working.* NGH-PO-236. Northampton. NGHT.

NHS Security Management Service (2009) '*Not alone' A guide for the better protection of lone workers in the NHS* [online] NHSBSA. Available from: http://www.nhsbsa.nhs.uk/SecurityManagement/Documents/Lone_Working_Guidance_final.pdf

APPENDICES

Appendix 1 **Security Environment and Asset Risk Assessment Tool**

Appendix 2 **Security poster to be displayed in staff areas**

Appendix 3 **Security Department Daily Lockdown timetable**

Security of Premises and Assets 2014
#NGH-PO-116-2014

Business Area
Facilities

Person Responsible
Clare Topping

Created
1st July, 2014

Last Review
1st July, 2014

Status
Complete

Next Review
3rd April, 2017

Screening Data

Name, job title, department and telephone number of the person completing this Equality Impact Assessment

> Clare Topping
> Energy and Sustainability Manager
> Facilities Department
> ex 5754

What is the title and number of this policy/procedure/guideline?

> Security of Premises and Assets
> NGH-PO-116

What are the main aims, objectives or purpose of this policy/procedure/guideline?

> Ensure security of confidential information, protection of property against loss, fraud, damage, detection of criminal offences.

Who is intended to benefit from this policy/procedure/guideline?

> All staff employed by NGH Trust as well as patients and visitors.

Is this a Trustwide, Directorate only or Department only policy/procedure/guideline?

> Trustwide

Who is responsible for the implementation of the policy/procedure/guideline?

> Deputy Hotel Services Manager / LSMS

Recommend this EA for Full Impact Analysis?

No

Comments

Policy applies equally across the Trust and does not affect any group more than others.

Rate this EA

Low

Organisation Sign-off Data

If the policy is implemented what is the potential risk of it having an adverse effect on equality?

Low Risk - probably will not have an adverse effect on equality

If the policy is implemented what is the potential of it having a positive effect on equality and relations?

Moderate Potential - may have the potential to promote equality and good relations

If the potential for risk or positive effect occurred what would be the potential number of people it effected?

A moderate amount of people would be affected

Based on the answers to questions 1 - 3 will this policy promote equality and diversity?

Yes

Policy sets out security details designed to protect staff, patients and their property as well as NGH property, this includes those considered most vulnerable.

Do you have any additional comments or observations about the policy?

No

How will the results of the Equality Impact Assessment will be published?

Within the text of the Policy

Have you completed any Action Boxes with recommended actions or changes for completion?

No

If 'Yes' please print off an action plan report along with a copy of the Equality Impact Assessment report to the policy/procedure/guidelines owner, and record below who it has been sent to

If 'No' please print off a copy of the Equality Impact Assessment report to the policy/procedure/guidelines owner, and record below who it has been sent to

Andy Watkins, Deputy Hotel Services Manager

Please give details of the monitoring arrangements

Will be reviewed at the next review of the policy

Next Review Date

2017-04-03

Outstanding Actions

No outstanding actions

Appendix 1

SECURITY ENVIRONMENT AND ASSET RISK ASSESSMENT TOOL
Northampton General Hospital NHS Trust

Directorate……..
Assessed by……. Date…….

Ward/Department /Area	Doors (locks, keys, coded swipe etc)	Windows (How secured)	Fire Escapes	CCTV Equipment	Any additional security measures	Insecurity identified YES/NO	Risk to area i.e. not able to secure area from public	Agreed Action	By Whom and When

- When carrying out an assessment start from the perimeter entrance points and work inwards where appropriate
- Refer to Security Policy 116 for further guidance

COMMENTS

Appendix 2

TO CONTACT SECURITY IN AN EMERGENCY DIAL

2222

APPENDIX 3

HOTEL SERVICES SECURITY DEPARTMENT

TRUST SITE LOCK –UP AND UNLOCK PROCEDURES

ROUND ONE - UNLOCK

TIME	LOCATION	AREA
5.00	PHASE ONE AUTOMATIC DOORS	D
	SOUTH ENTRANCE AUTOMATIC DOORS	D
6.00	GREEN FIRE DOOR – BOTTOM OF HOSPITAL STREET	N
	STAFF ONLY OUT OF HOURS DIGIT CODED DOOR	N
	STAFF ONLY OUT OF HOURS DIGIT CODED DOOR (TOP OF NORTH STREET)	R
	INTERAL DIGIT CODED CORRIDOR DOUBLE DOORS BY THE BOARDROOM	R
	GREEN FIRE DOOR TO ROBERTSON SUITE	R
	CEM FIRE DOOR	R
	MAXILLO FACIAL ENTRANCE OFF BILLING ROAD	R
	BILLING ROAD AUTOMATIC DOORS	T
	PUBLIC TOILETS (NEXT TO POSTROOM)	T
	SPENCER GARDENS	S
	COLPOSCOPY FIRE DOOR	S
	SPENCER WARD AUTOMATIC DOORS	S
	EYE TO EYE AUTOMATIC DOORS	L
	FIRE DOOR BY EYE DEPARTMENT	L
	INTERNAL CORRIDOR DOUBLE DOORS BY STURTRIDGE WARD	M
	INTERNAL CORRIDOR DOUBLE DOORS BY PADDINGTON WARD	M
	AREA K BUILDING AUTOMATIC DOORS	K
7.00	UNLOCK COMPLETE	

RED DENOTES DOORS NOT UNLOCKED AT THE WEEKEND

ROUND TWO - EVENING LOCK UP

18.00	INTERAL DIGIT CODED CORRIDOR DOUBLE DOORS BY THE BOARDROOM	R
	GREEN FIRE DOOR TO ROBERTSON SUITE	R
	CEM FIRE DOOR	R
	MAXILLO FACIAL ENTRANCE OFF BILLING ROAD	R
	SPENCER GARDENS	S
	WASTE BAY BASEMENT DOORS	E
	BASEMENT INNER SWIPE DOORS	E
19.00	CENTRAL PRODUCTION UNIT DOORS	E
	INTEGRATED SURGER LINK CORRIDOR DOOR	B
	AREA K AUTOMATIC DOORS (SECURE INTERNAL CORRIDOR DOORS	K

APPENDIX 3

ROUND THREE - NIGHT LOCK UP

21.00	GREEN FIRE DOOR – BOTTOM OF HOSPITAL STREET	N
	STAFF ONLY OUT OF HOURS DIGIT CODED DOOR	N
	ALTHORP WARD DOORS	S
	BILLING ROAD AUTOMATIC DOORS	T
	PUBLIC TOILETS SAT/SUN ONLY (NEXT TO POSTROOM)	T
	CHECK REAR DOOR TO CHIEF EXECUITVE CORRIDOR	S
	COLPOSCOPY FIRE DOOR	S
	SPENCER WARD AUTOMATIC DOORS	S
	EYE TO EYE AUTOMATIC DOORS	L
	FIRE DOOR BY EYE DEPARTMENT	L
	INTERNAL CORRIDOR DOUBLE DOORS BY STURTRIDGE WARD	M
	INTERNAL CORRIDOR DOUBLE DOORS BY PADDINGTON WARD	M
	PHASE ONE AUTOMATIC DOORS	D
	SOUTH ENTRANCE AUTOMATIC DOORS	D
22.00	LOCK UP COMPLETE	

During the evening Security will be contacted by Dermatology and Gynae Bureau staff and informed that Security can secure area. Both departments are located in Area K. In the event no contact is made Security will check and secure departments on round three lock up.

EMERGENCY SITE LOCKDOWN

There maybe a requirement to initiate a lockdown of the Trust site buildings outside of the set lock up time patrol. This may occur as a result of a significant or major incident. In the event of this the Trusts Local Security Management Specialist (LSMS) or Portering and Security Manager on authorisation from the Trusts Nominated Emergency Planning Officer (NEPO) or deputy will instruct Security Officers on duty to initiate a lock down.

Full Lock Down
On the instruction of a full lockdown secure all doors as per lock up procedure.

Partial Lockdown
Lockdown of the site may only require certain buildings and areas. The Trusts LSMS Portering and Security Manager or authorised senior manager will instruct Security Officers on duty on which doors and area to secure.

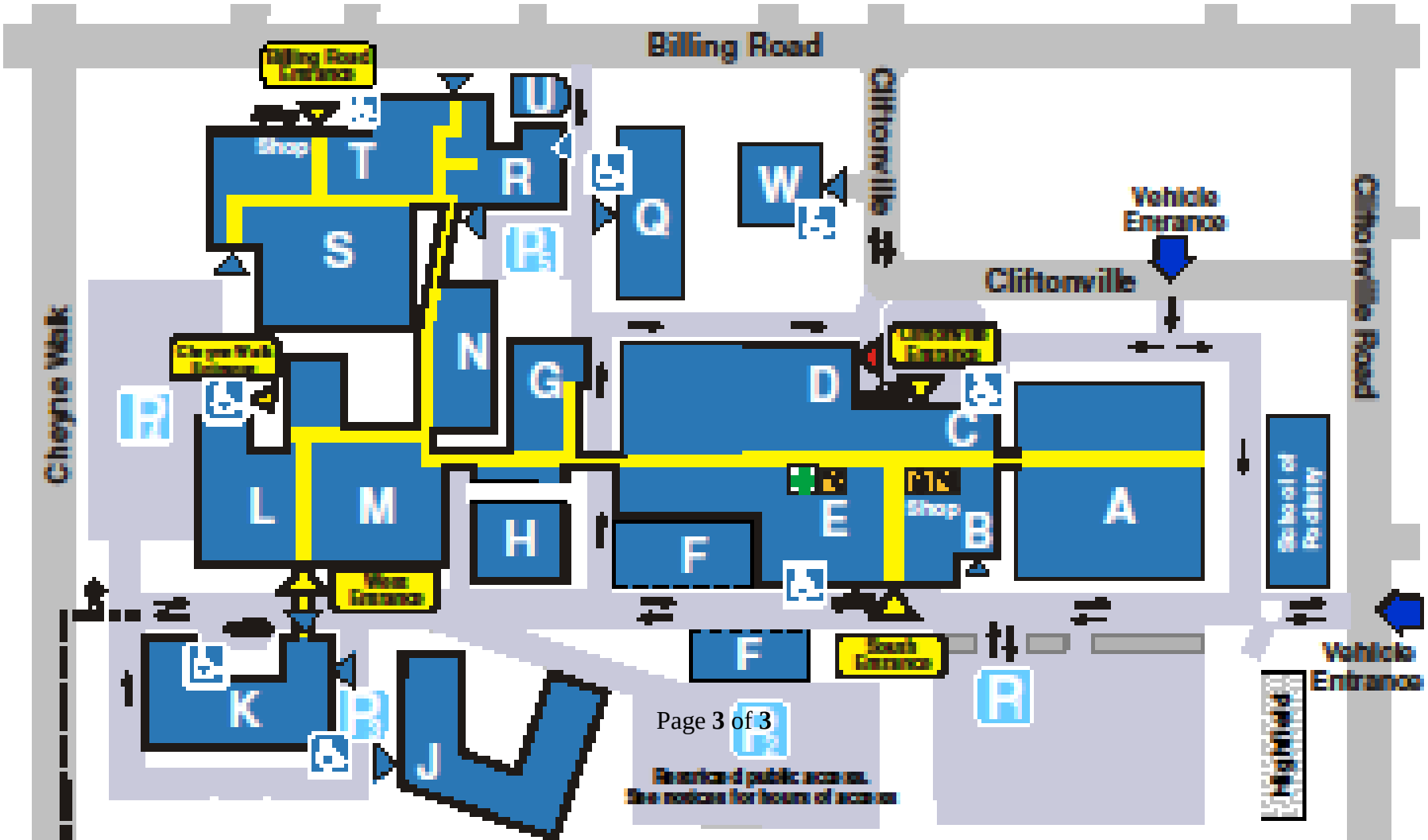
Stand down
The Trusts LSMS Portering and Security Manager or authorised senior manager will instruct Security Officers on duty when to stand down and initiate unlock patrol.

April 2010

APPENDIX 3

Northampton General Hospital

When you arrive at the hospital
please follow letters on signage to the area you require



Northampton General Hospital NHS
NHS Trust

FORM 1a- RATIFICATION FORM - FOR COMPLETION BY DOCUMENT LEAD Note: Delegated ratification groups may use alternative ratification documents approved by the procedural document groups.	
DOCUMENT DETAILS	
Document Name:	SECURITY OF PREMISES AND ASSETS
Is the document new?	No
If yes a new number will be allocated by Governance	N/A
If No - quote old Document Reference Number	NGH-PO-116
This Version Number:	**Version: 6**
Date originally ratified:	1999
Date reviewed:	June 2014
Date of next review: a 3 year date will be given unless you specify different	**June 2016 (2 Years)**
If a Policy has the document been Equality & Diversity Impact Assessed? (please attach the electronic copy)	Yes
DETAILS OF NOMINATED LEAD	
Full Name:	Andrew Watkins
Job Title:	Deputy Hotel Services Manager
Directorate:	Estates and Facilities
Email Address:	andrew.watkins@ngh.nhs.uk
Ext No:	5726
DOCUMENT IDENTIFICATION	
Keywords: **please give up to 10** – to assist a search on intranet	Security, Valuables, Safety, Secure, Alarms, Locked doors, Criminal Incidents

GROUPS WHO THIS DOCUMENT WILL AFFECT?
(please highlight the Directorates below who will need to take note of this updated / new policy)

Anaesthetics & Critical Care	Gynaecology	Medicine
Child Health	Haematology	Nursing & Patient Services
Corporate Affairs	Head & Neck - incl Ophthalmology	Obstetrics
Diagnostics	Human Resources	Oncology
Facilities	Infection Control	Planning & Development
Finance	Information Governance	Trauma & Orthopaedics
General Surgery		Trust wide

TO BE DISSEMINATED TO: NB – if Trust wide document it should be electronically disseminated to Head Nurses/ Dm's and CD's .List below all additional ways you as document lead intend to implement this policy such as; as presentations at groups, forums, meetings, workshops, The Point, Insight, newsletters, training etc below:

Where	When	Who

Northampton General Hospital NHS
NHS Trust

FORM 2 - RATIFICATION FORM to be completed by the document lead

Please Note: Document will not be uploaded onto the intranet without completion of this form

CONSULTATION PROCESS

NB: You MUST request and record a response from those you consult, even if their response requires no changes. Consider Relevant staff groups that the document affects/ will be used by, Directorate Managers, Head of Department ,CDs, Head Nurses , NGH library regarding References made, Staff Side (Unions), HR Others please specify

Name, Committee or Group Consulted	Date Policy Sent for Consultation	Amendments requested?	Amendments Made - Comments
Julie Quincey	29/04/2014	Can LSMS and SMD be full title when first used	Full titles stated when first indicated
Kared Qureshi	29/04/2014	7.5 change ext number from 5444 to5442	amended
Caroline Corkerry	29/04/2014	7.3 would read better if it said complete an incident report on the Datix system b) you may need to define or attach your criteria as an appendix for "investigate incidents when appropriate to do so" how do you decide what is appropriate to investigate & what is not? How is this applied consistently? Pg 18- Monitoring table needs some of the columns filling in	Included Statement removed Completed
Tony O'Donovan	29/04/14	Include this section Non Estates Contractors It is the responsibility of the Department requiring the contract work to be undertaken to ensure they are satisfied that they hold relevant insurance details, Risk Assessments & Method Statements, etc. to allow the work	Included

		to proceed at no risk to the Trust.	
Deborah Saberi	29/04/2014	P 17 refers to reporting incidents to line manager, should it also say something about reporting them onto Datix?	Included

Existing document only - FOR COMPLETION BY DOCUMENT LEAD		
Have there been any significant changes to this document? *if no you do not need to complete a consultation process*		NO
Sections Amended:	NO	**Specific area amended within this section**
Re-formatted into current Trust format	YES	
Summary/ Introduction/Purpose	NO	
Scope	NO	
Definitions	NO	
Roles and responsibilities	NO	
Substantive content	NO	
Monitoring	NO	
Refs & Assoc Docs	NO	
Appendices	NO	

FORM 3- RATIFICATION FORM (FOR PROCEDURAL DOCUMENTS GROUP USE ONLY) **Read in conjunction with FORM 2**					
Document Name:	**Security of Premises and Assets**		**Document No:**	**NGH-PO-116**	
Overall Comments from PDG re the Policy	**To return to PDG in June**				
	YES / NO / NA	**Recommendations**	**Recommendations completed**	**Recommendations**	**Recommendations completed**
Consultation Do you feel that a reasonable attempt has been made to ensure relevant expertise has been used?	**YES**				
Title -Is the title clear and unambiguous?	**YES**				
Is it clear whether the document is a strategy, policy, protocol, guideline or standard?	**YES**				
Summary Is it brief and to the point?	**NO**	Simplify Summary Add contacts into a table and include emergency number	Completed		
Introduction Is it brief and to the point?	**YES / NO / NA**	Reword first paragraph	Completed	REPLACE SMS with NHS protect	Completed
Purpose Is the purpose for the development of the document clearly stated?	**YES**				
Scope -Is the target audience clear and unambiguous?	**YES**				
Compliance statements – is it the latest version	**YES**				
Definitions –is it clear what definitions have been used in the	**NO**	Add SMS & LSMS, Assets, premises (including offsite) business visitors (as per the rewording in the substantive)	Completed		
Roles & Responsibilities Do the individuals listed understand about their role in managing and implementing the policy?	**YES / NO / NA**	Change management to line management	Completed		
Substantive Content is the Information presented clear/concise and sufficient?	**YES / NO / NA**	7.2 if 15 or above add 7.6 Reword the paragraph to make it more clear	Completed Completed	7.6 Reword first paragraph 7.10 Change Incidences and Incidents	Completed Completed
Implementation & Training – is it clear how this will procedural document will be implemented and what training is required?	**YES**				
Monitoring & Review (policy only) -Are you satisfied that the information given will in fact monitor compliance with the policy?	**YES**	Complete the monitoring and review table	Completed		

References & Associated Documentation / **Appendices**- are these up to date and in Harvard Does the information provided provide a clear evidence base? Are the reference provided using Harvard Referencing format?	**NO**	Please check the library references inserted into the reference section and address comments in red Remove appendix 1 this relates to violence and aggression not security of premises and assets Appendix 4 This is out of date T&D is locked at 6pm	Completed Completed there is no reference to this in lockdown schedule so not relevant	Check the appendices numbers throughout	Completed
Are the keywords relevant	**YES**				

Name of Ratification Group	Ratified Yes: **Ratified No: To go back to PDG**	Date of Meeting: **29/05/2014**
PDG		
Name of Ratification Group	Ratified Yes: subject to minor amendments and chair approval	Date of Meeting: **19/06/2014**
PDG		
Name of Ratification Group	Ratified Yes:	Date of Meeting: **26/06/2014**
Chair Approval		