Fareham & Gosport and
South Eastern Hampshire
Clinical Commissioning Groups

SECURITY POLICY - (STAFF, PREMISES AND ASSETS)

Subject and version number of document:	Security policy (staff, premises and assets) v1
Unique Reference Number:	COR/00x/Version 1.00
Operative date:	
Author:	Simon Zammit - Local Security Management Specialist
Review date:	
For action by:	All staff of the Clinical Commissioning Group ()
Policy statement:	This document sets out the policy by which the management of security, prevention and management of violence and aggression against staff and the protection of assets will be controlled. This is a corporate policy.
Responsibility for dissemination to new staff:	NH Business Development Manager
Training Implications:	
Further details and additional copies available from:	
Equality Analysis Completed?	Yes
Consultation Process	Due to the nature of this policy the Governing Body will be asked to approve and ratify the document.
Approved & ratified by:	Corporate Governance Committee
Date approved:	16 October 2015

Intranet and Website Upload: Intranet ONLY

Website	Intranet ONLY	September 2105
Keywords:	Security, Crime, Violence, Abuse, Theft, Assault, Protect, Assets, Premises, Staff	

Amendments Summary:

Amend No	Issued	Page(s)	Subject	Action Date
1				
2				
3				
4				
5				

Review Log:

Include details of when the document was last reviewed:

Version Number	Review Date	Name of Reviewer	Ratification Process	Notes
1.0	Aug 15	Simon Zammit		

SECURITY POLICY (STAFF, PREMISES AND ASSETS)

Contents

1.0 INTRODUCTION AND PURPOSE

1.1 Introduction

The CCGs recognise and accept their obligations relating to the management of security so far is reasonably practicable. Security of people, premises and assets within the CCGs is the concern of ALL of its members, employees and contractors. The CCGs will ensure that all possible measures are taken to deliver a properly secure environment for all who work for it.

The CCGs also have a responsibility to ensure that all services they commission on behalf of the local NHS are appropriately protected from crime and misuse. This is provided for in Service Condition 24 of the NHS Standard Provider Contract (2015). The arrangements will apply to providers as contracts are put in place or renewed.

1.2 NHS Protect

NHS Protect leads on work to safeguard NHS staff and resources from crime. It provides support, advice and guidance in this area to organisations across the NHS. NHS Protect works closely with NHS England to ensure organisations commissioning and providing NHS services meet nationally mandated standards in regard to anti-crime work.

1.3 Purpose

To provide local leadership within our areas of responsibility for NHS crime reduction and prevention work by applying an approach that is strategic, coordinated, risk and evidence based.

To work in partnership with the NHS England, NHS Protect and provider organisations, as well as non-health sector stakeholders, to coordinate the delivery of our work and to take action against those who commit offences against the NHS.

To establish a safe and secure environment that has systems and policies in place to: protect staff from violence, harassment and abuse; safeguard NHS property and assets from theft, misappropriation or criminal damage.

The CCGs provide for the day to day management of security through the post of Local Security Manager Specialist (LSMS).

2. SCOPE AND DEFINITIONS

2.1 Scope

This policy covers the security of staff and property within Fareham & Gosport and South Eastern Hampshire CCGs (the CCGs) and focuses on sustaining and improving existing physical and personal security.

The CCGs are committed to providing a safe and secure environment for their staff and visitors and to maintaining the security of its premises and assets.

The CCGs believe that effective security is an integrated function of all organisational activity. The responsibility for compliance with this policy is delegated to all employees to an extent consistent with their position. Put simply, Security is everyone's' business.

The CCGs' Security Policy supports the Policy and work of NHS Protect

2.2 Definitions

Arson – Causing deliberate or negligent damage to any property by means of fire

Burglary – Entering a building or part of a building without lawful authority and committing a criminal act (arson, theft, criminal damage, sexual assault).

Criminal Damage – Deliberate or negligent damage caused to any property or asset, includes vandalism and graffiti

Harassment - where a person or organisation is made to feel alarmed or distressed by another person's actions. The prosecution has to prove that a reasonable person would have known that the behaviour would create distress or fear. The harassment must have happened on at least two occasions.

Hazard - this is a natural or accidental situation that could cause harm (in terms of lone working, an example would be the absence of a functioning telephone)

LSMS – Local Security Management Specialist, (accredited trained person)

Non-Physical Assault – The use of inappropriate words or behaviour causing distress and/or constituting harassment.

Physical Assault – The use of physical violence against a person, without lawful justification, resulting in physical, psychological or emotional injury

Physical Security – The measures taken to either prevent a direct attempt to gain access to premises/assets or to reduce the potential damage and injuries that can be inflicted should an incident occur.

Risk – this is the likelihood versus the potential consequence of a hazard/threat causing harm.

Stalking - the name given to a form of harassment where an individual is made to feel alarmed or distressed by another person's actions.

Theft – taking someone else's property dishonestly, with the intention of never returning it. OR having permission to take something treats it as if the owner by disposing of it or lending it to a third party.

Threat – this is a person based issue that could cause harm (in terms of lone working, an example would be having to deal with a violent or abusive individual)

3.0 PROCESS / REQUIREMENTS

3.1 Risk Management

Risk management is to be at the heart of all security and crime prevention work. All risk management work is to comply with the provisions of the organisation's Risk Management Policy.

The LSMS will conduct a premises security risk assessment, which will be reviewed annually in June for the CCGs HQ.

Risk assessments will be undertaken in accordance with the CCGs' Risk Assessment Policy.

The Risk Manager will ensure that the risk assessment and any action plans are reviewed on an annual basis by the corporate governance committee. The LSMS annual and periodic reports will also include a review of the organisational action plan and a report on progress regarding its implementation.

ALL risk assessments will be properly recorded and retained in accordance with records retention policy.

3.1.1 Security Alerts

The LSMS will receive security risk alerts from NHS Protect and other Hampshire Health Sector Organisations. On receipt of these, they will assess the applicability of the identified risks to the organisation and its staff, forwarding the assessment and a recommendation of appropriate action to the Security Management Director. The SMD will make an executive decision as to whether to accept the assessment and recommended actions.

3.2 Managing Violent & Abusive Behaviour By Members Of The Public

Whilst assuming a zero tolerance stance regarding violence and aggression is desired it has been accepted nationally that this is not realistic. However, the CCGs will consider all incidents individually and with particular sensitivity, taking full account of, and support for, the wishes of victims as much as it is reasonably practicable in the circumstances.

All line managers and departmental heads need to ensure the following actions are carried out for all activities and locations:

- Role based risk assessments – must be formally recorded in accordance with the organisations Risk Management Policy.
- Implementation of risk mitigation/control measures, including staff training.
- The prompt reporting of ALL incidents of violence and aggression (verbal or physical).
- The wellbeing of the victim following an assault.
- All assaults on staff members are immediately reported to the police and LSMS
- That any member of staff who becomes a victim is fully supported and is referred for counselling – if necessary.

Part of the incident handling process should involve a root cause analysis and plans for prevention of repetition of the incident.

All employees must incorporate good working practices together with security measures as part of an overall requirement. The CCGs will have systems in place to ensure an appropriate response to incidents including:

- Recording all incidents on an effective database, whereby trends can be identified and risks assessed. - QUASAR
- Routine reports indicating trends and the needs for action to be taken in compliance with all relevant security policies

The CCGs are committed to reducing aggression against their staff and will consider measures to achieve this including:

- Instructor lead training in Conflict Resolution for all staff with regular contact with the public who are in role identified as being in a moderate or high risk role based on a formal documented risk assessment;
- E-learning based training in Conflict Resolution for all other staff
- The LSMS will speak on personal safety and security awareness at Team Training Days (as requested);

- On-going risk analysis by managers;
- Being supportive to staff identified as being at risk.
- Taking management action in line with the national framework of sanctions produced by NHS Protect.

3.3 Staff Support Following an Incident or Near Miss

The CCGs will fully support employees who report an incident. When an offence is committed against persons or NHS property within the CCGs and the culprit is identified, it is the policy of the CCGs to report the matter to the police and seek redress and/or sanction where appropriate. An Adverse Incident Report (AIR) must be completed for all incidents or near misses and recorded on QUASAR.

Employees are to report the full details to their appropriate manager/supervisor immediately before referral to any other agencies, e.g. Occupational Health, Human Resources, etc. (except in the case of incidents requiring an immediate Emergency Services presence or response).

The CCGs provide staff with access to a counselling service from Right Management. Information is available via their
website: www.wellness.rightmanagement.co.uk/login or
telephone 24/7 at 0800 1116 387.

Following an incident, managers must ensure that staff members are given the opportunity to discuss the incident and receive assistance in the preparation of reports on the incident.

Managers must arrange for staff to have time off to attend supportive agencies if required. Staff may wish to consult with their professional staff organisation or trade union or LSMS to obtain further advice and assistance.

3.4 Post Incident Investigations

After any incident of violence or aggression against an employee, line and service managers are to ensure that a root cause analysis is conducted and that a copy of the Risk Assessment for the task which was being under taken by the victim at the time is immediately forwarded to the LSMS.

3.5 Lone Working

Working alone is not prohibited by health and safety legislation and it will often be safe to work in this way. However, the law requires employers to consider carefully, and then deal with, any health and safety risks for people working alone.

The broad duties of the Health and Safety at Work Act 1974, the Management of Health and Safety at Work Regulations 1999, the Corporate Manslaughter and Corporate Homicide Act 2007, the Safety Representative and Safety Committees Regulations 1977, the Health and Safety (Consultation with Employees) Regulations 1996, apply.

These require the identification of hazards associated with lone working, assessment of the risks involved and putting in place measures to avoid or control the risks.

3.5.1 Lone Worker Risk Assessments

Risk assessments must be carried out by line managers with all staff as part of the induction process. The assessments must be recorded, re-examined at regular intervals and communicated to all who could be affected or identified by the risk

assessment. Re-assessment must take place annually as a matter of routine; more frequently in the event that there is a significant change in the individual's role and responsibilities, work base or disability / health status.

Measures to control the risks should take account of normal working conditions and foreseeable emergency situations such as fire, equipment failure, illness and accidents. When considering safe working arrangements, line managers should follow a hierarchical system based on the following:

- Identify who is operating as a lone worker;
- Identify any possible risk(s);
- Assess the likelihood and consequences of each risk;
- Avoidance of the risk where possible;
- Control of the risk as far as reasonably practicable;
- Evaluation and review of the effectiveness of control measures.

3.5.2 Office Based Lone Working

Where managers or employees are required to work alone in the organisation's headquarters, or other premises, they should ensure that where appropriate local premises management/security personnel are aware as are colleagues.

In locations where there is no premises management or security presence, they should ensure colleagues are aware of their late/lone working along with family members and ensure there is a process established to check on the welfare of the employee.

They are to take all reasonable steps to ensure their own safety, by ensuring access to their work areas are controlled so as only authorised persons may enter or leave.

On departure, lone workers are to ensure the offices are properly secure, and where appropriate any intruder alarm is set. Prior to exiting the secure area, they should look to see if there is any hazard or threat between them and their method of transport if practicable. They should notify their previously mentioned colleague and/or family member that they are about to leave and how long it is likely to be before they get home.

On arrival at their home or other place of safety, they are to ensure any work colleagues who have been their point of contact are made aware of their safe arrival.

3.5.3 Travelling Alone on CCG Business

Where staff are required to travel alone on CCG business, they are to ensure that their team colleagues are aware of the following information:

- If using a car, the make, model colour and registration of vehicle being used
- The route being taken
- The destination along with person(s) visiting
- Estimated time of departure
- Estimated time of arrival
- Purpose of visit.
- Any known risks.

Travellers are to ensure they check in with a colleague on departure and arrival at their destination as well as on leaving and safe return

3.5.4 Failure to return/respond to attempts to contact

Where staff attempt to make contact with a lone worker and there is no response, or, where a lone worker fails to return as expected, the following action is to be taken:

- Leave Voice message if possible requesting urgent contact.
- After 15 minutes with no response escalate to head of department,
- Call home address and enquire after colleague – do not hint at any problems.
- HoD to contact Duty Executive Member.
- Make decision to call police.

3.6 PHYSICAL SECURITY

3.6.1 Security of buildings and offices

All buildings and offices are to be fully secured when not in use. Desks are to be cleared at the end of each day and pedestals are to be locked. No keys are to be left insecure.

3.6.2 Visitors/Contractors

All contractors and visitors to CCGs' premises for business purposes should be signed in and out of the premises. There will be a visitor log held at the reception area. The member of staff who is responsible for the visitor/contractor will then arrange for the visitor to be escorted at all times whilst on the premises.

3.6.3 Staff Identification

This policy requires that all staff display their CCG identification badges while at work. Staff members are to ensure their badges are visible at all times while at work.

Failure to display a valid I.D. badge <u>may</u> result in disciplinary action being taken.

3.6.4 Challenging persons not displaying a valid ID Badge

Any unescorted person who is seen not wearing a visible CCGs ID badge whom is found in any non-public area should be challenged. A polite but assertive challenge should be all that is required for that person to identify themselves, such as, 'Can I help you?' Suspicious behaviour should be reported to your manager and the LSMS.

3.6.5 Provision of Security Systems

The CCGs are responsible for funding any security measures at premises that is solely beneficial to the organisation and would be sited within the boundaries of its tenancy.

The landlord is responsible for all whole site security and any measures intended to protect multiple tenants.

Should the CCGs identify the need for additional measures within its areas, the LSMS must be asked to produce an "operational requirement" prior to any liaison with the landlord.

3.7 Security Incidents & Reporting Process

The CCGs expect that patients, clients, relatives and any users of its services will behave in a manner that respects its staff while providing care in a patient's home

or premises. The CCGs will not tolerate any form of violence or abuse of staff, visitors and property. Behaviours that are unacceptable within the CCGs include:

- Violence including assaults
- Threatening or abusive language
- Threats or threatening behaviour
- Damage to CCGs' property
- Derogatory, racial or sexual remarks
- Repetitive vexatious complaints
- Theft
- Anti-Social Behaviour

3.7.1 Reporting Process

On receipt of any report of any of crime or security incident, individuals/managers are to raise an incident report on QUASAR. **In addition** they are to inform the LSMS by e-mail within 24 hours of the incident. The LSMS will provide advice and guidance on appropriate responses in accordance with this policy.

3.8 Security of Assets

A register of all business critical assets should be created and maintained irrespective of value.

The asset register is to be kept secure and only authorised persons allowed access to it and see its contents.

Details recorded within the asset register should include:

- Make and Model – all details about the item available at receipt of purchase.
- Description – full description of the item being recorded
- Serial numbers of the item(s)
- Location / department where the item(s) are located

Where possible all assets should be indelibly marked with a unique reference number.

This provision does not apply to information or IT assets which are covered in the relevant policies.

3.9 Fire Safety

The overlapping interests of security and fire safety policies are fully recognised and there will be full cooperation between the Fire Safety Officer and the LSMS in regard to physical security of premises.

3.10 Counter Terrorism

Whilst there is no evidence to suggest that the NHS is any more at risk from terrorism than other public service organisations, staff should maintain a level of alertness commensurate with the fact that many patients in the CCGs area will be members of military families. Counter terrorism guidance can be found on the MI5 and Centre for Protection of the National Infrastructure websites. www.mi5.gov.uk and www.cpni.gov.uk

3.10.1 Telephone Bomb Threats

Making such malicious calls is an offence contrary to Section 51 of the Criminal Law Act 1977 and should always be reported to the police. The procedure in the Premises Security Plan must be used in event of the organisation receiving such a call:

In all cases it is important to telephone the police immediately with details of the call.

The message may be brief and the caller may ring off before detailed information can be obtained. However, try and obtain what information you can, such as detailed in the Premises Security Plan. The four key rules are:

- Keep calm.
- Try to obtain as much information as possible from the call.
- Keep the line open even after the caller has hung up.
- Report the call to your manager.

This is easier said than done. Do not underestimate the stress of receiving a threatening call - it can put the best intentions out of mind until the caller has rung off and it is too late to try to get more details.

If at all possible, the person receiving such a call should signal to a colleague to listen in on the same extension. Another person listening on the line may help to remember important facts afterwards.

- Keep the caller talking for as long as possible.
- Complete the questionnaire in the CCGs Security Procedure as soon as possible.
- Try to ask questions in sequence using as natural a voice as possible.
- Remember **DON'T HANG UP**

4. ROLES AND RESPONSIBILITIES

4.1 The CCGs Governing Bodies

The CCGs Governing bodies are responsible for ensuring that legal obligations are met in line with the risk management agenda and that resources are made available to ensure that the premises are maintained in a physical secure condition.

4.2 Security Management Director (SMD)

An SMD will be nominated to take overall responsibility for all aspects of Local Security

Management matters, with priority for dealing with matters of violence against staff, ensuring measures to address the following areas are implemented:

- Lone worker safety
- Prevention and management of violence and aggression against staff
- Protection of assets, medications prescription forms and hazardous materials

The current SMD is the Chief Financial Officer

4.3 Heads of Department

It is the responsibility of all Heads of Department to:

- Communicate the content and requirements of the Security Policy within the area of their responsibility
- Ensure the implementation of the Security Policy within the area of their responsibility by providing support and advice to their managers.
- Co-ordinate security issues with other employers who share the worksite with the CCGs

4.4 Hampshire and Isle of Wight Fraud and Security Management (HIoWF&SMS)

The Security Management Service sits within the above team hosted by North Hampshire. It supplies the Local Security Management Specialist, and as such this organisation provides services to the CCGs.

4.5 Local Security Management Specialist (LSMS)

The nominated Local Security Management Specialists (LSMS) are to provide professional skills and expertise to tackle security management issues across a range of proactive and reactive action. The overall objective of the LSMS will be to work on behalf of the CCGs to deliver an environment that is safe and secure so that the highest standards of clinical care can be made available to patients.

4.6 Risk Manager

The Risk Manager is responsible for ensuring that all security related Adverse Event Reports are notified within 24hrs of receipt (Mon – Fri) to the LSMS and for providing a copy of the individual forms. The Risk Manager has responsibility for ensuring that all received security incidents are registered on the CCGs QUASAR database and for providing information to the LSMS on trends and incidents

4.7 Health & Safety Advisor

The Health & Safety Advisor is responsible for working with the LSMS to ensure that H&S aspects of security incidents are dealt with in the appropriate manner.

4.8 Team Managers

The team managers have an overview of matters relating to security, violence prevention and personal safety within their own area and will work with the LSMS to ensure the operational implementation of the Security Policy.

They will:

- Work with the LSMS to improve all aspects of security within their own areas by supporting, where practicable, all security improvements recommended by the LSMS
- Work with the LSMS to ensure that security surveys for all the CCGs premises are carried out, recorded and appropriately acted upon.
- Liaise with managers and departmental heads in matters of security as appropriate

4.9 All Managers

Security is the responsibility of all managers and departmental heads who must undertake preventative measures for the safety of staff and property. It is their job to see that the right policies, procedures and systems are in place in their local areas and that such policies are kept under constant review. They will carry out risk assessments and ensure that staff are trained and receive relevant instruction and training.

It is the individual manager and responsibility to ensure that safe and secure environments are maintained and that all incidents are fully reported and that action is taken when necessary. They are to inform the LSMS of all security incidents immediately on being notified. This is to be followed up by a confirmatory e-mail. This is to contain full details of the incident.

Managers are to implement a procedure to record details i.e. make, model, serial number etc. of all valuable or important property within their Department. The LSMS can advise on methods to secure property.

They should also:

- Ensure that arrangements are made to secure the Department out of working hours together with the safe custody of keys.
- Ensure the correct use of any security system or device to protect the property out of hours.
- Ensure records are kept of all keys issued to staff in their Department and reporting all losses of keys to their Head of Department.
- Seek advice from the LSMS to ensure that the highest standard of security is maintained within their Department.
- Ensure all staff employed by the CCGs, staff from other organisations working in the CCGs' offices, wear an ID badge at all times, visitors should not be left unescorted.
- Ensure that all staff are made aware of this Security Policy and fully understand its content and their responsibilities.
- Ensure that future job descriptions for all managers include, as part of their duties, the responsibility for security within their department.
- Managers need to assess the impact on security of new projects and proposed changes to services.

4.10 Responsibilities of the Employee

Security is the responsibility of all employees and they are expected to co-operate with management to achieve the aims, objectives and principles of the security policy. Great emphasis is placed on the importance of co-operation of all staff in observing security and combating crime.

Where employees become aware of actual or potential breaches of security, all such incidents must be reported in accordance with the CCGs' Incident Reporting Policy

All staff must recognise the responsibility they have for the confidentiality of the information they hold and use, in particular patient information. They must comply with all local departmental procedures and protocols that ensure the security of that information and prevent it being compromised.

All employees are reminded that it is an offence to remove (or borrow) any the CCGs property without written agreement from their departmental manager. Failure to do so could result in disciplinary action and/or criminal proceedings being taken.

Employees are responsible, at all times, for the protection and safe keeping of their private property. Any loss, theft or damage to private property from the CCGs premises or while the staff member is on duty should also be reported.

5. TRAINING

The CCGs recognise the need for effective training of staff to deal with security related issues and will, through the CSU South Learning and Department and the LSMS, ensure security advice and training, is provided with regard to:

- Conflict Resolution Training to reduce the likelihood of assault.
    - This is mandatory training for all employees who deal with the public
- Crime reduction and prevention within the working environment;
- Responding promptly and effectively to all criminal events.

6. SUCCESS CRITERIA

That all CCGs services have been considered for issues relevant to the organisational action plan through monitoring and receipt of Risk Assessments by the LSMS

The Annual Self Review Tool and Work Plan and LSMS' interim reports will be reviewed on a quarterly basis by the Audit committee.

The LSMS, through the SMD is to present an annual report to the CCG Board highlighting the year's activities and achievements and identifying challenges for the coming year

7. REFERENCE DOCUMENTATION

Health and Safety at Work Act 1974. London: The Stationary Office.

NHS Counter Fraud and Security Management Service (2005) *Safe and Secure. How you can help the NHS Protect itself.* NHS CFSMS.

NHS Counter Fraud and Security Management Service. (2003). *A professional Approach to Managing Security in the NHS.* NHS CFSMS

NHS Counter Fraud and Security Management Service (2005) NHS Security Management

Manual NHS Protect

NHS Protect website: www.nhsbsa.nhs.uk/protect

Associated CCG policies

Risk Management Policy

Emergency Planning

Incident Reporting Policy

Health & Safety Policy

Lone Working Policy

8. EQUALITY IMPACT ASSESSMENT

The Clinical Commissioning Groups are committed to equality of opportunity for all people and to eliminate unlawful discrimination (Equality and Diversity Strategy 2014/15). As part of its development, this policy and its impact on staff, service users and the public has been reviewed in line with the CCGs' legal equality duties due regard to eliminate discrimination, harassment and victimisation, to advance equality of opportunity, and to foster good relations between people who share a relevant protected characteristic and those who do not share it (as cited in the Equality Act 2010) has been given throughout the development of this policy.

Employees, contractors and visitors of different ages, genders, those with a range of disabilities, and women who are pregnant or new mothers are identified as most likely to be impacted upon. Particular attention has therefore been made in this policy to remove or reduce any potential negative equality impact.

There is also a need to monitor the protected characteristics of employees, contractors and visitors who are involved in security incidents or who report risks and concerns. This will enable responsible managers and the CCGs to identify any trends and take further necessary action.

9. MONITORING AND REVIEW

This policy will initially be reviewed after 12 months and then on a three yearly rolling basis however it may be reviewed earlier in line with new guidance and with reference to Adverse Event Data, prosecution progress and Risk Assessment findings.