NHS
Rotherham
Clinical Commissioning Group

Title:	**Policy & Procedure for the Management of Security (including Lone Working Procedure)**
Reference No:	C12
Owner:	Operational Executive
Author	Sarah Whittle/Ruth Nutbrown Reviewed by Ian Plummer
First Issued On:	July 2016
Latest Issue Date:	September 2019
Operational Date:	September 2019
Review Date:	July 2022
Consultation Process	OE – 21/06/2019 AQuA – 02/07/2019 GB – 04/09/2019
Ratified and approved by:	Governing Body
Distribution:	All staff and GP members of the CCG.
Compliance:	Mandatory for all permanent and temporary employees of Rotherham CCG.
Equality & Diversity Statement:	In applying this policy, the Organisation will have due regard for the need to eliminate unlawful discrimination**,** promote equality of opportunity**,** and provide for good relations between people of diverse groups, in particular on the grounds of the following characteristics protected by the Equality Act (2010); age, disability, gender, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, and sexual orientation, in addition to offending background, trade union membership, or any other personal characteristic.

CONTENTS

1. Introduction

NHS Rotherham Clinical Commissioning Group (CCG) is committed to a safe and secure environment that protects staff, patients and visitors, and their property and the physical assets of the CCG, via Health and Safety legislation, Department of Health Policy and by a common law duty of care. This policy aims to deal proactively with the CCG's security arrangements.

2. Purpose

The purpose of this policy is to ensure that wherever possible effective measures are taken to:

- Protect the safety, security and welfare of staff, patients and the general public whilst on CCG premises.
- Provide systems and safeguards against crime, loss, damage or theft of property and equipment.
- Minimise disruption or loss of service to patients/clients.

It is the CCG's intention to take all reasonable practicable steps to reduce the associated risks from security issues.

The CCG will also ensure, so far as is reasonably practical, that all employees who are required to work alone for significant periods of time are protected from risks to their health and safety.

3. Definitions

a) NHS Counter Fraud Authority

The NHS Counter Fraud Authority (NHSCFA) is a special health authority charged with identifying, investigating and preventing fraud and other economic crime within the NHS and the wider health group.

b) Local Security Management Specialist (LSMS)

The Local Security Management Specialist (LSMS) is highly trained by NHS Counter Fraud Authority and will be involved in performing a wide range of security-related tasks:

- Creating a 'pro-security' culture amongst staff, professionals and the public
- Deterring those who may be minded to breach security
- Preventing security incidents or breaches from occurring
- Detecting security incidents and reporting them to NHS Counter Fraud Authority
- Investigating security incidents in a fair, objective and professional manner
- Applying a wide range of sanctions against those responsible for security incidents, involving a combination of procedural, disciplinary, civil and criminal action as appropriate
- Seeking redress through the criminal and civil justice systems against those whose actions lead to loss of NHS resources
- To deter Criminal activities where possible by putting in place essential security control systems and other counter measures

- To deny the criminal opportunity, not only through physical barriers, but by putting in place effective systems of loss prevention and property control
- To detect the criminal act. The earlier the criminal act is detected and reported the greater the chances of preventing the offenders absconding. Raised awareness of security at all levels will both detect and reduce the risk of crime
- To respond effectively to security issues and problems with workable counter measures
- To review the strategy after every incident, also after counter measures have been put in place to evaluate their effectiveness
- To liaise with the local police and the local authority to achieve partnership working towards a safe and secure environment

The Local Security Management Specialist will work closely with the Local Counter Fraud Specialist to prevent and detect crime and fraudulent activities.

c) Property

Can be defined as the physical buildings in which NHS staff and professionals work, where patients are treated and from where the business of the NHS is delivered.

d) Assets

Assets, irrespective of their value can be defined as the materials and equipment used to deliver NHS healthcare. In respect of staff, professionals and patients it can also mean the personal possessions they retain whilst working in, using or providing services to the NHS.

e) Premises

Premises are land and buildings together considered as a property.

4. Duties

a) Chief Officer

Overall accountability for ensuring that there are systems and processes to effectively manage security lies with the Chief Officer who takes the risks to the CCG from breaches of security seriously and seeks to reduce the numbers of incidents occurring as a direct result. The Chief Officer also functions as the Security Management Director.

Responsibility is also delegated to the following individuals.

b) Assistant Chief Officer

The Assistant Chief Officer has lead responsibility for the development and strategic review of Security within Rotherham CCG, in line with the Secretary of State's Directions of November 2003.

The Assistant Chief Officer is responsible for:

- The formulation, implementation and maintenance of an effective Security Policy, (following NHS Counter Fraud Authority guidance) in consultation with staff

representatives, and ensuring that Managers co-ordinate and implement the Policy in their respective areas.

- Reviewing and amending this policy to ensure compliance with any current guidance.
- Instituting regular campaigns to highlight the importance of security and the responsibilities of all CCG staff.
- Leading Security Management within the CCG and identifying security initiatives for improving the security across the CCG.
- Advising the CCG of any requirements, statutory or other, by the preparation of procedures for dealing with crime prevention, supply of security systems and maintenance.
- Monitoring the performance of the CCG with regard to the implementation of this policy.

c) <u>Local Security Management Specialist (LSMS)</u>

The nominated Local Security Management Specialist (LSMS) for the CCG is the Assistant Chief Officer. The overall objective of the LSMS will be to work on behalf of Rotherham CCG to deliver an environment that is safe and secure.

This objective will be achieved by working in close partnership with stakeholders within Rotherham CCG, NHS Counter Fraud Authority and external organisations such as the police, professional representative bodies and trade unions. The LSMS will aim to provide comprehensive, inclusive and professional security management services for Rotherham CCG and work towards the creation of a pro-security culture within the NHS.

The LSMS will:

- Report to Rotherham CCG Security Management Director (SMD) on security management work locally.
- Lead on the day to day work within the CCG to tackle violence against staff and professionals in accordance with national guidance.
- Ensure that lessons are learned from security incidents, and that these incidents are assessed and the impact on the CCG reported to appropriate authorities in accordance with guidelines issued by NHS Counter Fraud Authority.
- Investigate security incidents/breaches in a fair, objective and professional manner so that the appropriate sanctions and consideration of preventative action can be taken.
- Ensure that the security management policy addresses all the organisations identified risks and contains all the required elements from NHS Counter Fraud Authority guidance.
- Ensure that the security management policy is reviewed or evaluated to establish its effectiveness.
- Ensure that any corrective or preventative actions identified as a result of the policy review or evaluation, are implemented to ensure that the security management policy continues to address the CCG's identified risks.

d) Other Chiefs of Service

Other Chiefs of Service, on behalf of the Chief Officer are responsible for ensuring that the CCG's Security Policy is implemented within the organisation. This will include responsibility for:

- Planning any capital investment required to address matters arising from risk assessments.
- Security risk assessment within their areas and for ensuring that staff for whom they are responsible are aware of these risks.
- Preventative measures and appropriate action in respect of persons who are suspected of committing a criminal offence, misconduct or other breach of security in contravention of the policies of the CCG.
- Ensuring staff awareness of, and how to access this policy and other relevant documents and their responsibilities and also ensure that staff (including temporary staff) receives training appropriate to the risks involved.
- Ensuring that security arrangements within their area are being observed and those deficiencies are reported.
- Ensuring that any particular security problems known to them are reported accordingly.
- Actively reviewing the security arrangements within their area by carrying out routine audits themselves with the co-operation of staff organisations, in line with CCG risk assessment procedures.
- Ensuring that every member of staff obtains a security ID Badge and that the badge is worn and visible at all times whilst the staff member is on CCG premises or on CCG business.
- An ongoing commitment to staff training, carrying out risk assessments, identifying areas at greatest risk and eliminating or controlling these risks.

e) Line Managers

Line Managers are responsible for:

- Ensuring compliance with CCG Security Policy requirements in the areas for which they are responsible.
- The completion of any risk assessments required in relation to security of staff or premises.
- Ensuring that any security problems known to them are reported accordingly.

f) Staff

Responsibilities of Staff (including all employees, whether full/part time, agency or bank) are:

- To co-operate with management to achieve the aims and objectives of the Security Policy. Great emphasis is placed on the importance of co-operation of all staff in observing security and combating crime.
- The protection and safe keeping of their personal property. Any loss of personal property must be reported without delay. If personal property has been stolen, then it is the owner's responsibility, not the CCG's responsibility to contact the Police.

- To familiarise themselves with:
    - any special security requirements relating to their place of work or work practices
    - the action to take in the event of a security incident
- To safeguard themselves, colleagues, visitors, patients/clients etc., so far as is reasonably practicable, and ensure that neither equipment nor property are put in jeopardy by their actions or omissions, either by instruction, example or behaviour.
- To follow prescribed working methods and security procedures at all times.
- To co-operate with managers to achieve the aims of the Security Policy.
- To comply with all training requirements concerning security issues.
- To ensure that the CCG ID is worn and visible whenever on CCG premises or on CCG business.
- To notify their line manager of any potential security problems and report all incidents involving criminal activity to the appropriate manager.
- To report any crime/breach of security (Appendix 1).

All staff are reminded that it is an offence to remove property belonging to the CCG without written authority. Failure to seek authority from their line manager could result in disciplinary action or criminal proceedings being taken.

NHS Rotherham CCG will not accept liability for the loss of, or damage to personal property including motor vehicles or other modes of transport. Motor vehicles are brought onto the sites entirely at the owner's risk.

5. Training

Part of the requirement for the effective implementation of a security management system is the training of all staff (including temporary staff) in security awareness.

The awareness training will cover the importance of conformance to the Security Policy, significant security effects, roles and responsibilities for security management functions, and the consequences of non-conformances.

Security awareness training will be integrated into induction training and into any mandatory ongoing training programmes as required based on risk assessments.

The CCG will ensure that appropriate information, instruction and training is given to employees who may be required to work alone, to ensure that so far as is reasonably practicable a safe system of work is in operation. Training will include physical security of assets and premises, and personal safety of staff.

Frontline Staff need to undergo Conflict Resolution Training and attend refresher training on a 3 yearly basis, as well as preventing and reporting crime in the workplace. This mandatory training must be included in departmental programmes as part of in-service training, and with periodic refresher courses. Training involves dealing with situations of potential or actual abuse, aggression of violence, and includes:

- understanding the causes;
- recognising the warning signs;
- identifying when and where to get help;

- interpersonal skills/defusing techniques.

6. Committee Responsibility for Security Management

Committees and Sub Committees of the Governing Body have delegated responsibility for security management according to the scheme of delegation detailed below. These Committees and Sub Committees should ensure that relevant consultation on planned changes has been undertaken with relevant groups prior to reaching decisions around security matters.

Body	Type of responsibility
OE	Has a responsibility to monitor the effectiveness of this policy and ensure resources are available to support the implementation of associated control measures via regular updates from the Corporate Assurance Report on incident statistics. Where it is not possible to address certain risks, the OE has the ultimate responsibility for the acceptance of those risks.
AQuA	The AQuA Committee is responsible for the monitoring, through the Corporate Assurance Report, the effectiveness of: • Security management • Risk assessments • Security action plan.
GB	The GB has the overall responsibility for the monitoring and reporting of security management work.

7. Monitoring & Review

The procedural document will be reviewed every three years, and in accordance with the following, on an as and when required basis:

- Legislative changes
- Good practice guidelines
- Case Law
- Significant incidents reported
- New vulnerabilities identified
- Changes to organisational infrastructure
- Changes in practice

Procedural document management will be performance monitored to ensure that procedural documents are in-date, effective and relevant to the core business of the CCG. The results will be published in the regular Corporate Assurance Reports.

SECURITY MANAGEMENT PROCEDURE

1. Rehabilitation of Offenders Act 1974

All persons applying for a post within the CCG must have completed the section on the application form entitled Rehabilitation of Offenders Act 1974. This section states that 'because of the nature of the work for which you are applying, this post is exempt from provisions of Section 4(2) of the Rehabilitation of Offenders Act, 1974 (Exemption) Order, 1975.' Applicants are therefore, not entitled to withhold information about convictions which for purposes are 'spent' under the provisions of the Act, and in the event of employment, any failure to disclose such convictions could result in dismissal or disciplinary action by the CCG.

This application form also requests details of any convictions, adult cautions or bind-overs, and requires the applicant to sign the statement confirming that the information given is correct. For more information refer to the Recruitment and Selection Policy

2. Children Act 1989

In accordance with the provisions of the Children's Act 1989, the CCG must ensure that staff who occupy certain positions which bring them regularly in contact with children have a criminal record check. An application for a Criminal Records Disclosure will be requested following appointment of the staff member by the Human Resources Department.

3. Personal Security

Specific procedures for local needs such as domiciliary visits (e.g. lone workers), staff in other premises, agile workers etc. are to be developed and implemented by individual departments. All staff must follow existing Health & Safety policies and guidelines.

4. Staff Identification

Every employee including bank staff, will be issued with an identification badge on commencement of employment which must be worn at all times whilst on CCG premises or on official CCG business.

Each member of staff is personally responsible for their badge, and to ensure that the badge is up to date. If there are changes in physical appearance, title or department, it is the responsibility of the member of staff to inform the Corporate Business Team who will issue a new ID badge.

Identification badges must be returned to the Corporate Business Team when a member of staff leaves the employment of the CCG. It is the responsibility of the senior manager completing the exit interview to recover the identity badge and access fob from the member of staff concerned.

All members of staff should challenge any person within the CCG demised area who is not known and without an ID badge.

5. Funding

Each Department must take into account security issues including cost implications when:

- Developing schemes for minor improvements
- Developing schemes for new premises, major upgrading etc.

- Introducing new services or changes to existing services, which may have implications for staff security.

6. Key Holding

The responsibility for the arrangements for daily opening/closing premises rests with the Security Management Director (SMD). This includes the maintenance of a key register which identifies the location of all keys. The register should detail the individuals in receipt of keys and signatures should be obtained.

7. Access and Egress

Access to NHS Rotherham CCG premises will be restricted. The responsibility for the arrangements to access the demised areas rests with the Corporate Business Team.

8. Security of Goods

Goods delivered to Oak House are checked against delivery notes prior to signing for acceptance. The Landlord provides secure accommodation on reception for goods awaiting distribution.

All CCG departments receiving goods must ensure there are procedures in place to monitor the receipt of goods and safe /secure systems are in place to protect goods from theft or inappropriate use.

9. Security of Personal Belongings

All staff should ensure that personal belongings are stored in a secure location e.g. locked in cupboards or desk drawers. The CCG cannot be held responsible for theft of personal items that are not secured.

10. Fraud

The responsibilities for fraud prevention are described in the CCG Fraud, Bribery and Corruption Policy.

The LSMS will liaise regularly with the Local Counter Fraud Specialist to ensure a direct and close relationship is maintained.

Any suspicions of fraud, bribery or corruption should be reported directly to the CCG's Counter Fraud Specialist.

11. Fire

The overlapping interests of security and fire safety policies are fully recognised and there is full co-operation between fire and security staff.

12. Information Security

The objective of information security is to ensure faith in the bond of confidentiality between the CCG and its patients/clients and staff. It aims to ensure business continuity and minimise business damage by preventing and minimising the impact of security incidents.

All information is held in accordance with the CCG Information Governance Policy and

Management Framework.

13. Harassment, Violence and Aggression

Any member of the public or patients who abuse NHS Rotherham Clinical Commissioning Group staff may have sanctions taken against them, be refused treatment, or taken to court by the CCG.

For any occurrences of harassment, violence and aggression by staff to other members of staff or Service users / members of the public please follow the guidance contained within the Acceptable Standards of Behaviour Policy and Disciplinary Policy

13.1 Harassment:

The Citizens Advice defines Harassment as: When someone behaves in a way which offends you or makes you feel distressed or intimidated. This could be abusive comments or jokes, graffiti or insulting gestures**.** Harassment occurs when someone is deliberately abused, threatened and/or humiliated. This may occur either inside or outside working hours.

13.2 Violence:

The Health and Safety Executive (HSE) defines violence as: Any incident in which a person is abused, threatened or assaulted in circumstances relating to their work.

Violence is the intentional use of physical force or power, threatened or actual, against oneself, another person, or against a group or community, that either results in or has a high likelihood of resulting in injury, death or psychological harm, this may occur either inside or outside working hours.

13.3 Both harassment and violence may be carried out to staff by service users or members of the public with the purpose or effect of violating a manager's or staff member dignity, affecting his/her health and/or creating a hostile work environment.

13.4 Harassment and violence can:

- Be physical, psychological, and/or sexual.
- Be amongst colleagues, between managers and staff or by third parties such as service users, patients etc.
- Range from minor cases of disrespect to more serious acts, including criminal offences, which require the intervention of public authorities.
- This can occur in the work environment or outside the work environment.

13.5 Harassment can be further defined as any conduct which:

- Is unwanted by the recipient
- Is considered objectionable by the recipient
- Causes humiliation, offence and distress (or other detrimental effect)

The key to distinguishing between what does and does not constitute harassment is that harassment is behaviour that is unwanted by the person to whom it is directed. It is the

impact of the conduct and not the intent of the perpetrator that is the determinant.

Harassment is a course of conduct which may occur against one or more individuals, harassment may be, but is not limited to:

- Physical contact – ranging from touching to serious assault, gestures, intimidation, aggressive behaviour
- Verbal – unwelcome remarks, suggestions and propositions, malicious gossip, jokes and banter, offensive language
- Non-verbal – offensive literature or pictures, graffiti and computer imagery, emails, texts, isolation or non- co-operation and exclusion or isolation from social activities
- Unwanted conduct related to a protected characteristic under the Equalities Act 2010 which has the purpose or effect of violating an individual's dignity or creating an intimidating, hostile, humiliating or offensive environment for that individual.

13.6 Aggression

- Hostile, injurious, or destructive behaviour or outlook especially when caused by frustration, aggression can be an expression of pent-up rage.
- Spoken or physical behavior that is threatening to the individual and or involves harm to someone or something.

13.7 Assessing the risk of violent behaviour

Violent incidents do not necessarily have to cause physical harm. They can:

- Involve a threat, even if no serious injury results.
- Involve verbal abuse.
- Involve non-verbal abuse, for example gestures, emails, texts.

In any situation where physical assault is considered imminent, staff should immediately leave the area if able and contact security (if available) or the police (9-999 from an internal phone or 999 from a mobile).

13.8 The process for staff following violent or abusive behaviour from service users or members of the public:

All instances of actual or threatened harassment, violence and aggression from service users or members of the public must be reported to your line manager. The line manager will need to consider whether the matter should be referred to the Police.

Incidents of violence and aggression can have a detrimental effect on the victim out of proportion to the scale seen by outsiders. Managers are to ensure that members of staff are supported as soon as is reasonably practicable after such incident(s).

It is important that an investigation into the matter is conducted and members of staff are informed of the basic details of the incident and any counter measures planned to prevent a similar occurrence.

Rotherham CCG will make training available in the management and handling of violence and aggression, based on the training needs analysis. In any cases where a member of staff feels that a service user or member of the public has behaved in an inappropriate

manner, the line manager must be informed of the occurrence and a report completed as soon as reasonably practicable.

13.9 Dealing with harassment, violence and aggression pro-actively

Staff should attempt to avoid physical intervention at all costs and be aware of their own verbal and non-verbal communication. Conflict Resolution Training (CRT) is available to members of staff.

Techniques include:

- Simply ask the person who is becoming aggressive to stop; some people will respond to this.
- Attempting to establish a rapport.
- Offering and negotiating realistic options.
- Avoiding threats.
- Asking open questions and asking about the reason for the service user's concern(s).
- Showing concern and attentiveness through non-verbal and verbal responses.
- Listening carefully to the service user.
- Attempting to neither patronise nor minimise the service user's concerns.

13.10 Possible warnings which may indicate an individual's behaviour is escalating towards physically violent behaviour includes but not limited to:

- Direct prolonged eye contact
- Facial colour may darken / go pale
- Head drops to protect throat
- Lips tighten over teeth
- Eyebrows droop to protect eyes
- Breathing rate accelerates
- Fists clenching and unclenching
- Subject stands tall, attempting to intimidate
- Behaviour may stop/start abruptly
- Kicking the ground
- Large movements close to people
- Hands rise above waists
- Shoulders tense
- Stance moves from square to sideways
- Lowering of body to launch forward

13.11 Dealing with harassment, violence and aggression reactively

Dependent on the circumstances, in an incident involving harassment, violence and aggression, the following course of action (13.12) could be pursued in conjunction with any

other course of action, but always in consultation with Senior Management. Any and all action must be fully and factually documented and an incident report form completed.

13.12 Actions following violent or abusive behaviour

Where a patient, relative or member of the public is alleged to have carried out an act of violence, abuse or aggression then the CCG reserves the right to respond to the alleged incident, as deemed necessary in light of the circumstances. The level of response will be dependent upon the seriousness of the incident and the outcome of any investigation. The potential responses or actions available to the CCG include:

- Verbal warnings with a follow up letter to the individual
- Recommendation to use advocacy services
- Warning flag applied to patients notes
- Meeting with the individuals
- Written warnings from the CCG
- Withdrawal of services
- Involvement of the Local Security Manager
- Involvement of the police
- Criminal prosecution
- Civil Prosecution

13.13 Dealing with actual or threatened violence and aggression could have an effect on an employee's health and wellbeing, and they may feel that they need further support with this. Rotherham CCG is committed to the health and well-being of staff, and has therefore put in place an employee assistance programme (EAP) to provide additional support where needed. The EAP will offer employees a variety of support services, including financial, legal, education, consumer and family care advice as well as access to 24 hours a day, 7 days a week health advice lines, staffed by qualified pharmacists and nurses. In addition to this, the programme will also offer staff free access to counselling services. Staff, when experiencing an issue where they feel counselling would be beneficial will be able to contact the employee assistance provider and have up to 5 face to face counselling sessions. The counselling lines are open 24 hours a day 7 days a week.

14. Major Incident

A major incident is a serious unforeseen occurrence using disruption to the normal life of the CCG happening suddenly with little or no warning and causing or threatening death or serious injury to staff and members of the public; damage or destruction of property which necessitates special mobilisation and organisation. Please refer to the Emergency Preparedness, Resilience and Response Policy.

15. Risk Assessment

The Management (Health, Safety and Welfare) Regulations 1999 (Regulation 3) require that suitable and sufficient risk assessments be undertaken, so that the significance of a hazard can be identified, assessed and controlled. Guidance on assessing risks to safety and health can be found on the HSE website (http://www.hse.gov.uk/simple-health-safety/risk/index.htm).

It is the responsibility of the appropriately trained Managers within the CCG to see that these are carried out, and a copy of the assessment forwarded to the LSMS. The LSMS will keep a record of the assessment carried out and ensure they are reviewed yearly or sooner if he/she is required to do so.

If the risk is deemed serious by the LSMS the risk assessment will be forwarded for inclusion on the CCG's Risk Register.

Risk Assessments should be completed for all security hazards including physical (buildings, equipment etc.) and people. These risk assessments are the responsibility of the department involved, with support from the LSMS where required.

Risks relating to security are identified on an ongoing basis through incident reports, complaints and claims procedures.

It is important that all staff within the CCG are aware of the security risks involved within their work. They must also be aware of formal risk assessments that apply to them, the actions identified to control the risks and the measures to be taken by them personally to reduce the risks to themselves and others.

When working arrangements are agreed with an individual which result in that person working alone for regular/significant periods, then the manager will be responsible for ensuring that a risk assessment is undertaken and that a related safe system of work is put in place. This will take into account the capability of the individual. The employee will be required to conform to these arrangements, to safeguard both themselves and the CCG.

Working alone is not illegal, but it can bring additional risks to a work activity. The CCG has developed policies and procedures to control the risks and protect employees, which employees should know and follow them. Apart from the employee being capable of undertaking the work/detail the three most important aspects to be certain of are that:

- The lone worker has full knowledge of the hazards and risks to which they are exposed.
- The lone worker knows what to do if something goes wrong.
- Someone else knows the whereabouts of the lone worker and what he/she is doing.

For further guidance please refer to the CCG's Lone Working Procedure (appendix 2).

Reporting of Crime/Security Incidents

All staff has a responsibility to report any crime/breach of security. This reporting falls into the following categories:

1. Rotherham CCG Premises - Oak House

When a crime/security incident of a serious nature is taking place dial 999 and report the incident to the police, and follow their advice. You must then contact the Security Management Director or their Deputy and inform them of the incident.

Where a security/criminal incident is discovered, the information must be passed to the Security Management Director or their Deputy and the LSMS as soon as practicable.

Complete an Incident Reporting Form (as per Incident Policy) and forward a copy to the Local Security Management Specialist.

1.1 External Locations

When a crime/security incident of a serious nature is taking place, you should call the police immediately by telephoning 999.

Where a security incident is discovered, the information should be passed to the Security Management Director or their Deputy as soon as practicable.

Complete an Incident Reporting Form (as per Incident Policy) and forward a copy to the Local Security Management Specialist.

1.2 Out of Hours – Oak House

When a crime/security incident of a serious nature is taking place, you should call the police immediately by telephoning 999.

Following this; the incident should be reported to the Security Management Director or their Deputy as soon as possible.

1.3 Suspicious (suspect) packages

- A suspect package is a package believed to contain a potentially harmful device or substance.
- Any suspect package (postal item, e.g. letter / package) when received must immediately be placed in isolation (and not moved again) and away from water, chemicals, heated surfaces, naked flames and gaseous substances. It is more likely to be an incendiary device than a bomb; i.e. it is designed to start a fire.
- Do not shake it, squeeze, or open the letter or package.
- Turn off all air conditioners, fans, photocopiers, printers, computers and heaters within the room where the letter / package is located if possible. Close all windows and evacuate the room, close all doors. Place a clearly visible warning on the door.
- Any suspicious packages (other items e.g. bags, boxes that have appeared) should NOT be moved and its position should be reported to the Security Management Director or their Deputy or a member of the Senior Management Team. Undertake initial investigation (without touching or moving the package) identifying:

- ❖ The listed owner of the package
- ❖ Visible wires or electrical components showing from the package, especially where the wrapping has been damaged
- ❖ Any greasy marks on the envelope or package
- ❖ If an unknown powder or liquid substance is leaking from the package
- ❖ Distinctive smells from the package e.g. almonds / marzipan or machine oil
- ❖ If the package when delivered was heavy for its size or has an uneven distribution of weight or has excessive wrapping
- ❖ If the package was delivered by hand from an unknown source or posted from an unusual place

- If in doubt, dial 999 and report to police and evacuate the building without sounding the fire alarm and closing doors and windows behind you.
- Do not use mobile telephones near suspect packages.
- If you feel you may have been contaminated by substances leaking from the package, go to an isolated room and avoid other people if you can. It is vitally important that you segregate yourself and others who may have come into contact with the suspicious package. It is unlikely that you have been contaminated and you will get medical treatment if required. Signs that people may have been exposed to a chemical incident are streaming eyes, coughs and irritated skin. Do not rub your eyes; touch your face or other people. Thoroughly wash your hands / face in soap and water as soon as possible.
- Where convenient, fire assembly points can be utilised for the purpose of evacuation, but only if they are located at a distance of at least 400 metres from the suspected bomb site. Safe assembly points are best situated behind a solid building at a distance away from the blast site.

1.4 Bomb threats

- A bomb threat is a threat to detonate an explosive or incendiary device to cause property damage or injuries, whether or not such a device actually exists. Bomb threats are usually made verbally over the phone.
- Notification of a bomb threat can be made at any time and can be made and delivered by several means, usually anonymous, but all must be considered seriously.
- Any member of staff receiving a telephone threat regarding a suspect package or explosive device should obtain as must detail as possible from the caller. The police need to be informed immediately - dial 999 and report to police and evacuate the building without sounding the fire alarm; closing doors and windows behind you. Report the situation to the Security Management Director or their Deputy or a member of the Senior Management Team who will decide whether an emergency should be declared in line with the Emergency Preparedness, Resilience & Response Policy.

Appendix 2

NHS Rotherham CCG Lone Working Procedure

1. Introduction

This procedure sets out the steps the CCG will take to keep lone workers; healthy and safe.

Working alone is not in itself against the law and it will often be safe to do so. However, the law requires employers to consider carefully, and then deal with any health and safety risks for people working alone, including any contractors or self-employed people doing work for the CCG. These responsibilities cannot be transferred to any other person, including those people who work alone.

This procedure applies to all staff who work for NHS Rotherham CCG who may Lone work.

2. Definitions

The Health and Safety Executive (HSE) defines lone workers as:

"Those who work by themselves without close or direct supervision"

Further HSE definition examples include lone workers who work by themselves without close or direct supervision such as:

- only one employee works on the premises
- employees work separately from others
- employees work outside normal hours

It is recognised that any employee may spend a limited amount of their working time 'alone'.

3. Principles

Lone workers should not be put at more risk than other employees. Establishing a healthy and safe working environment for lone workers can be different from organising the health and safety of other employees.

The CCG should take account of normal work and foreseeable emergencies, e.g. fire, equipment failure, illness and accidents and identify situations where people work alone and consider the following:

- Does the workplace present a specific risk to the lone worker?
- Is there a safe way in and out for one person, e.g. for a lone person working out of hours where the workplace could be locked up?
- Is there a risk of violence and/or aggression?
- Are there any reasons why the individual might be more vulnerable than others and be particularly at risk if they work alone (for example if they are young, pregnant, disabled or a trainee)?
- If the lone worker's first language is not English, are suitable arrangements in place to ensure clear communications, especially in an emergency?

4. Procedure

4.1 Members of staff and persons working on behalf of the CCG working alone are at greater

risk for a number of reasons:

- Persons attending work early in the morning are potentially at risk because they are the first to enter the site or building, which could expose them to either danger from a fault such as gas leak or electrical fault which has developed over night
- There is increased threat of personal attack from unauthorised persons on site
- If a lone worker suffered an accident while working alone in the building there is a possibility that they would not be discovered for some time.

4.2 In order to mitigate these threats the following steps should be taken:

- The worker should obtain their line manager's agreement before working outside their normal hours
- The worker and their line manager should agree a procedure to allow the lone worker to be able to contact their line manager or a colleague in the case of an emergency
- When working late, the worker should inform their line manager beforehand if possible and also when they leave the premises
- If the line manager is not available, the worker should inform another manager or colleague of what time they expect to finish work and inform them if there are any changes to those plans. When the worker has finished and is outside the building, they should inform their contact that they are done for the day.
- Lone workers should always ensure they will be able to leave the office safely after working late.

4.3 Lone workers who are in the office either early morning or late evening should:

- Ensure they have immediate access to a telephone in order to call for help
- Identify potential escape routes including fire exits
- Ensure windows and doors are secured from unauthorised access
- Park in a well-lit area as close to the building as possible.

4.4 Staff working alone at other locations or out of hours:

- Lone workers must always ensure their electronic diaries are up to date and contain details of any off-site meetings including: Length of meeting, full postal address of venue and contact number. Electronic diaries should be open to all CCG staff.
- In instances where electronic diaries have appointments that contain sensitive or confidential information, these entry's should be made private in the diary and information shared with either a CCG manager or appropriate colleagues who have authorisation to view that level of information.
- Lone workers must always ensure that a CCG manager or appropriate colleague is aware of their planned movements. This means providing them with the address of where they will be working, details of the people they will be working with or visiting, telephone numbers if known and expected arrival and departure times.
- Arrangements must be in place to ensure that if a colleague with whom details have been left leaves work, they will pass the details to another colleague who will check that the lone worker arrives back at their office/base or has safely completed their duties. Procedures must also be in place to ensure that the lone worker is in regular contact

with their manager or relevant colleague, particularly if they are delayed or have to cancel an appointment.

- When working at other sites lone workers should ensure they understand the local procedures for locking up, times etc. They should always ensure that they sign out of the building.
- If they must work late they should ensure that their presence is reported to the proper person and that security (if applicable) is aware of the arrangements.
- All line managers are to ensure they have identified the staff in their teams who may Lone Work at other locations or out of hours.

5. Safe System of Work for Members of Staff

- All staff within the team will fully open their diaries to other members of the team.
- The intrinsic security of the building must not be compromised by lone workers, e.g. security doors will not be propped open, other people who should not be on the premises will not be brought on the premises by lone workers, etc.
- Full contact details of all off site working and meetings including full addresses of the venue, any applicable accommodation and full names, addresses (if applicable) and telephone/email addresses of contacts and other attendees to be notated in the diary entry.
- Mobile phones to be in use at all times the staff member is lone working, to be able to alert others or to summon help if required.
- If attending meetings at home addresses, contact should always be made with people with knowledge of the person meeting so a risk assessment can be completed if required.
    - If the risk assessment deems it necessary, procedures such as attending in two's, open communication whilst in the meeting etc. should be implemented.
- ICE (In Case of Emergency) contact to be incorporated in the mobile phone.
- If agreed, personal mobile phone numbers to be shared within the team.
- Informal buddy system to be put in place with definite timescales for escalation noted.
- Escalation procedure to be implemented if required.

6. Lone working and vehicles:

- Before setting out, lone workers should ensure that they have adequate fuel for their journey and give themselves enough time for the journey to avoid rushing or taking unnecessary risks.
- Items such as bags or cases should never be left visible in the car. These should be out of sight, preferably stored in the boot of the vehicle.
- Lone workers should always try to park close to the location that they are visiting and should never take short cuts to save time. At night or in poor weather conditions, they should park in a well-lit area and facing the direction in which they will leave. They should ensure that all the vehicle's windows are closed and the doors locked.
- In case of vehicle breakdown or accident, lone workers should contact their manager or colleague immediately. If they need to leave the vehicle to use an emergency

telephone, they should put their hazard lights on, lock their vehicle and ensure that they are visible to passing traffic.

7. Incidents and Reporting

Where an incident occurs, all staff are required to contact their immediate line manager and report the incident as documented in the CCGs Incident Management Policy located on the CCG website. (http://www.rotherhamccg.nhs.uk/quality-policies.htm)

8. Escalation Procedure

- Line managers must discuss with their lone worker staff what actions they should take in the event of an incident.
- Where there is genuine concern, as a result of a lone worker failing to attend a visit or an arranged meeting within an agreed time, or to make contact as agreed, the manager should use the information provided to locate them and ascertain whether they turned up for previous appointments that day. Depending on the circumstances and whether contact through normal means can be made, the manager or colleague should involve the police, if necessary.
- If it is thought that the lone worker may be at risk, it is important that matters are dealt with quickly, after considering all the available facts. If police involvement is needed, they must be given full access to information held and personnel who may hold it, that information might help trace the lone worker and provide a fuller assessment of any risks they may be facing.
- It is important that contact arrangements, once in place, are adhered to. Many such procedures fail simply because staff forget to make the necessary call when they finish their work. The result is unnecessary escalation and expense, which undermines the integrity of the process.

8.1 If a staff member is lone working and has been out of contact with their buddy for 1 hour after the expected timed response the following procedure will be undertaken:

- Contact with the staff member via mobile phone (corporate and personal if applicable), text message and email to be made. If no response within 15 minutes escalation to senior manager to be initiated and personal contact details to be requested from HR.
- Contact to be made with next of kin or ICE (In Case of Emergency) contact details held on file. If contact unsuccessful or negative response gained. Senior manager to make decision to escalate to Police.

9. References

The Health & Safety Executive has provided guidance related to lone working in the following publication:

- Working Alone: Health and Safety Guidance on the Risks of Lone Working http://www.hse.gov.uk/pubns/indg73.pdf
- Violence at Work. http://www.hse.gov.uk/pubns/indg69.pdf
- Preventing Workplace Harassment and Violence. http://www.hse.gov.uk/violence/preventing-workplace-harassment.pdf

Appendix 3

Checklist for the Review and Approval of Procedural Document

To be completed and attached to any document which guides practice when submitted to the appropriate committee for consideration and approval.

Display Screen Equipment Policy	YES/NO/Unsure	Comments
1. Title		
Is the title clear and unambiguous?	Yes	
Is it clear whether the document is a guideline, policy, procedure/protocol or plan?	Yes	
2. Rationale		
Are reasons for development of the document stated?	Yes	
3. Development Process		
Is the method described in brief?	No	
Are people involved in the development identified?	Yes	
Has relevant expertise has been used?	Yes	
Is there evidence of consultation with stakeholders and users?	Yes	
4. Content		
Is the objective of the document clear?	Yes	
Is the target population clear and unambiguous?	Yes	
Are the intended outcomes described?	Yes	
Are the statements clear and unambiguous?	Yes	
Are cross references accurate?	Yes	
5. Evidence Base		
Is the type of evidence to support the document identified explicitly?	Yes	
Are key references cited?	Yes	
Are the references cited in full?	Yes	
Are supporting documents referenced?	Yes	
6. Approval		
Does the document identify which committee/group will approve it?	Yes	
If appropriate have the joint Human Resources/staff side committee (or equivalent) approved the document?		