NHS
Barnsley
Clinical Commissioning Group

Barnsley Clinical Commissioning Group

Security Policy and Procedure

Version:	Approved v1.0
Approved By:	Governing Body
Date Approved:	August 2015, reviewed December 2017
Name of originator / author:	Richard Walker/Ruth Nutbrown Reviewed by Ian Plummer
Name of responsible committee/ individual:	Health & Safety Group
Name of executive lead:	Richard Walker
Date issued:	October 2018
Review Date:	3 years from date of approval
Target Audience:	All CCG Staff

DOCUMENT CONTROL

Version No	Type of Change	Date	Description of change
v0.1	Document developed	April 2015	*New document*
V0.2	Drafting changes	July 2015	*Minor changes following review of the original draft by Head of Assurance and Management Team*
V0.3	Drafting changes	August 2015	*Further minor drafting amendments*
V1.0	Approved version	August 2015	*Version approved by Governing Body on 13th August 2015*
V1.1	Minor amendments	November 2016	*1. Change of named Executive lead Vicky Peverelle to Richard Walker* *2. Change of named Security Management Director from Chief of Corporate Affairs to Head of Governance and Assurance* *3. Reference to Yorkshire and Humber Commissioning Support removed and replaced by South Yorkshire and Bassetlaw Clinical Commissioning groups* *4. Reviewed and updated the Lone working Risk Assessment (Appendix 4)* *5. Reviewed and updated the Equality Impact Assessment (Appendix 5)*
V1.2	Procedural Review	August 2017	*Minor changes to the wording of Appendix 1 & 2*
	Procedural review	November 2017	*Addition of information regarding the process when dealing with violence and aggression by service users or their families (Section 6.13)*
	Procedural review	December 2017	*1. Reference to NHS Protect (appendix 1) Changed to The NHS Counter Fraud Authority* *2. Minor changes to the wording of the Policy*

BARNSLEY CLINICAL COMMISSIONING GROUP

Security Policy and Procedure

Contents

1. Introduction

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

1.1.1 BCCG acknowledges its responsibility for the safety of people within the organisation and wider, and the requirement to have a written statement of general policy under the statutory requirements of:

- the Health and Safety at Work Act 1974
- NHS Protect guidance "Standards for Commissioners"

1.1.2 The Security policy has been developed in accordance with BCCG's Policy on the Development and Management of Policies and Procedures

1.1.3 This policy needs to be read in conjunction with the:

- Corporate Manual
- Fraud, Bribery and Corruption Policy
- Fire Safety Policy
- Health and Safety Policy

2. Purpose

2.1 BCCG recognises its responsibilities to ensure that reasonable precautions are taken to provide a safe and secure working environment and that steps are taken to prevent issues in relation to security management, in compliance with relevant statutes and codes of practice (as identified above).

2.1.1 In pursuance of this aim, BCCG will:

- Protect the safety, security and welfare of staff, patients and the general public whilst on BCCG premises
- Provide systems and safeguards against crime, loss, damage or theft of property and equipment
- Minimise disruption or loss of service to patients/clients
- Ensure Risk Assessment and security audits are implemented to comply with statute.

2.1.2 BCCG recognises that this Policy Statement is implemented in pursuance of these aims.

3. The Risks of not having this Policy in place

3.1 Not having this policy in place exposes BCCG to increased risk of failure to meet its legal responsibility to provide a safe and secure environment that protects staff, patients and visitors, and their property and the physical assets of BCCG.

4. Principles

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

4.1.1 BCCG 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.

5. Roles and Responsibilities

5.1 Security is a management responsibility and the provision of a security service in no way relieves management at any level of its obligations to fulfill the stated purpose of security in BCCG. Managers are required not only to exercise preventative aspects but also to take appropriate action where necessary in respect of those who offend against the law, commit misconduct or other breach of security in contravention of the policies of BCCG.

5.2 Overall accountability for ensuring that there are systems and processes to effectively manage security lies with the Chief Officer who takes the risks to BCCG from breaches of security seriously and seeks to reduce the numbers of incidents occurring as a direct result. Responsibility is also delegated to the following individuals:

5.2.1 The **Head of Governance and Assurance** functions as the Security Management Director and has lead responsibility for the development and strategic review of security within BCCG, in line with the Secretary of State's Directions of November 2003.

The Security Management Director 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 BCCG staff
- Leading Security Management within BCCG and identifying security initiatives for improving the security across BCCG
- Advising BCCG 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 BCCG with regard to the implementation of this policy.

5.2.2 The Competent Person for Security for BCCG is the Head of Specialist Advice, Health and Safety (South Yorkshire and Bassetlaw Clinical Commissioning Groups shared services). The overall objective will be to work on behalf of BCCG to deliver an environment that is safe and secure.

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

The Competent Person for Security will:

- Report to BCCG Security Management Director (SMD) on security management work locally.
- Lead on the day to day work within the BCCG 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 BCCG reported to appropriate authorities.
- Investigate security incidents/breaches in a fair, objective and professional manner so that the appropriate sanctions (and allow consideration of preventative action to be taken).
- Ensure that the security management policy addresses all the organisations identified risks and contains all the required elements from 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 evaluations are implemented, to ensure that the security management policy continues to address the CCG's identified risks.

5.2.3 Other Chiefs of Service, on behalf of the Chief Officer are responsible for ensuring that BCCG'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 BCCG
- 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) receive training appropriate to the risks involved
- Ensuring that security arrangements within their area are being observed and that 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 BCCG 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 BCCG premises or on BCCG business
- An ongoing commitment to staff training, carrying out risk assessments, identifying areas at greatest risk and eliminating or controlling these risks.

5.2.4 Line Managers are responsible for:

- Ensuring compliance with BCCG 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

5.2.5 Responsibilities of Staff (including all employees, whether full / part time, agency, bank or volunteers) 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 private property. Any loss of private property must be reported without delay. If private property has been stolen, then it is the owner's responsibility, not BCCG'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 BCCG ID is worn and visible whenever on BCCG premises or on BCCG 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. This procedure is documented as Appendix 2.

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

NHS Barnsley CCG will not accept liability for the loss of, or damage to private property including motor vehicles or other modes of transport. Motor vehicles are brought onto the sites entirely at the owner's risk. NHS Barnsley CCG will take reasonable steps to safeguard vehicles on their property.

6. Procedure

6.1 Employment

6.1.1 All persons applying for a post within BCCG 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 BCCG and referral to the Counter Fraud Specialist for further investigation. .

6.1.2 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 & Selection Policy.

6.1.3 In accordance with the provisions of the Children's Act 1989, BCCG must ensure that, staff who occupy certain positions that brings them regularly in contact with children have Disclosure & Barring Service check which will be requested as appropriate following appointment of the staff member by the Human Resources Department.

6.2 Personal Security

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

6.2.2 The requirement for security personnel (e.g. static or mobile guards) should be assessed by local managers and managed within each Department. The Competent Person for Security can advise and help manage arrangements if so required.

6.3 Staff Identification

6.3.1 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 BCCG premises or on official business.

6.3.2 Each member of staff is personally responsible for their badge, and to ensure that the badge is up to date and that there are no radical changes in physical appearance, title or department. All staff should wear an official BCCG identification badge and it is the responsibility of each departmental manager to ensure that this is implemented. The identity badge will state the employee name and job title and must be clearly visible to other staff, and visitors.

6.3.3 Identification badges must be returned to the Human Resources Department when a member of staff leaves the employment of BCCG. It is the responsibility of the line manager to recover the identity badge from the member of staff concerned and return it to the HR Department.

6.3.4 For the Management of Contractors please refer to the Control of Contractors Procedure.

6.4 Cash Movement/Handling

6.4.1 Only the Finance Team should hold cash, which will be managed in accordance with the Petty Cash Procedure.

6.5 Funding

6.5.1 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.

6.6 Key Holding

6.6.1 The responsibility for the arrangements for daily opening / closing of 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.

6.7 Access and Egress

6.7.1 Access to NHS Barnsley CCG premises will be restricted. The responsibility for the arrangements for daily opening / closing of premises and individual departments rests with the SMD.

6.7.2 Where appropriate, access will be controlled by the use of digital locks, electronic alarm systems and access to keys.

6.7.3 All windows at ground level, where appropriate, will be fitted with security devices or restrictors limiting the extent to which they can be opened.

6.7.4 The Security Management Director will put in place measures to ensure that locking systems and alarm codes are reviewed on a regular basis.

6.8 Security of Goods

6.8.1 Goods received into the organisation must be checked against delivery notes prior to signing for acceptance. The organisation will provide secure accommodation for goods awaiting distribution.

6.8.2 Some BCCG goods are received by South and West Yorkshire Partnership Foundation Trust (SWYPFT). These goods will remain the responsibility of SWYPFT until signed for by a BCCG staff member.

6.8.3 All BCCG 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.

6.9 Security of Personal Belongings

6.9.1 All staff should ensure that personal belongings are stored in a secure location e.g. locked in cupboards, lockers or desk drawers. NHS Barnsley CCG cannot be held responsible for theft of personal items.

6.10 Fraud, Bribery and Corruption

6.10.1 The responsibilities for fraud prevention and investigation are described in BCCG's Fraud, Bribery and Corruption Policy. The Competent Person for Security will liaise regularly with the Counter Fraud Specialist to ensure a direct and close relationship is maintained.

6.11 Fire

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

6.12 Information Security

6.12.1 Information security risk is inherent in all administrative and business activities and everyone working for or on behalf of NHS Barnsley CCG continuously manages information security risk. The aim of information security risk management is not to eliminate risk, but rather to provide the structural means to identify prioritise and manage the risks involved in all our organisational activities. It requires a balance between the cost of managing and treating information security risks with the anticipated benefits that will be derived.

6.12.2 All information is held in accordance with BCCG's Information Governance Strategy Framework, Policy and associated procedures. Further information can be found in the organisation's Information Security Management Statement and Assurance Plan.

6.13 Violence and Aggression

6.13.1 Any member of the public or patients who abuse NHS Barnsley Clinical Commissioning Group staff may have sanctions taken against them, be refused treatment, or taken to court by BCCG. For situations which involve members of staff who abuse members of the public or patients, please refer to the Acceptable Standards of Behaviour Policy.

6.13.2 Harassment and Violence:

The Health and Safety Executive (HSE) defines harassment and violence as unacceptable behaviour by one or more individuals that can take many different forms, some of which may be more easily identifiable than others.

Harassment occurs when someone is repeatedly and deliberately abused, threatened and/or humiliated. This may occur either inside or outside working hours Violence occurs when someone is assaulted in circumstances relating to work, this may occur either inside or outside working hours. Both may be carried out by one or more manager, staff, service user or member 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.

6.13.3 Harassment and violence can:

- Be physical, psychological, and/or sexual.
- Be amongst colleagues, between superiors and subordinates or by third parties such as clients, customers, 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.

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 which has the purpose or effect of violating an individual's dignity or creating an intimidating, hostile, humiliating or offensive environment for that individual.

6.13.4 Aggression

- a forceful action or procedure (such as an unprovoked attack) especially when intended to dominate or master
- hostile, injurious, or destructive behaviour or outlook especially when caused by frustration aggression is often the expression of pent-up rage
- spoken or physical behaviour that is threatening to the individual and or involves harm to someone or something

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.

Involve other threatening behaviour, for example stalking,

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).

6.13.5 Processes for staff following violent or abusive behaviour from service users or members of the public

All instances of actual or threatened violence and aggression must be reported in accordance with the

BCCG Incident Reporting Policy. Incident reporting will be used to ensure that other members of staff benefit from shared experiences and training can be realistic and relevant.

Staff that has been subjected to violent / abusive behaviour from service users or members of the public should report such incidents to their 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 staff are supported as soon as is reasonably practicable after such incident(s). Staff and Managers who are not directly involved could also be subject to anxiousness and concern.

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

6.13.6 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. E- Learning 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 through neutral communication;
- offering and negotiating realistic options;
- avoiding threats;
- asking open questions and asking about the reason for the service user’s concern;
- showing concern and attentiveness through non-verbal and positive verbal responses;
- listening carefully;
- attempting to neither patronise nor minimise the service user’s concerns

BCCG will make training available in the management and handling of violence and aggression to those staff who may require it. 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 an Incident Form completed as soon as reasonably practicable.

6.13.7 Dealing with harassment, violence and aggression reactively

Dependent on the circumstances, in an incident involving harassment, violence and aggression, the following course of action (6.13.8) 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.

6.13.8 Actions following violent, abusive or aggressive behaviour

Where a patient, relative or member of the public is alleged to have carried out an act of violence, aggression or harassed a member of staff, BCCG 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 BCCG 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
- Support mechanisms

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. BCCG 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 and are staffed by qualified counsellors and psychologists.

6.14 Emergency Preparedness, Resilience & Response

6.14.1 A significant incident or emergency can be described as any event that cannot be managed within routine service arrangements. Each requires the implementation of special procedures and may involve one or more of the emergency services, the wider NHS or a local authority. Please refer to the Emergency Preparedness, Resilience & Response Policy for further details.

6.15 Risk Assessment

6.15.1 The Management of Health and Safety at Work 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 in BCCG's guidance document – Risk Assessment Matrix. Please refer to the Integrated Risk Management Framework, Strategy, Policy and Procedure for further information.

6.15.2 Risks associated with security should be reported to the Competent Person for Security.

6.15.3 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 Competent Person for Security where required.

6.15.4 Risks relating to security are identified on an ongoing basis through incident reports, complaints and claims procedures, and the risk assessment procedure.

6.15.5 It is important that all staff within BCCG is 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.

6.15.6 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 NHS Barnsley CCG.

6.15.7 Working alone is not illegal, but it can bring additional risks to a work activity. BCCG has developed policies and procedures to control the risks and protect employees, and 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

7. Monitoring the Compliance and Effectiveness of this Policy

7.1 The Health and Safety Group will be responsible for monitoring compliance with, and the effectiveness of, this policy. In discharging this responsibility the Health and Safety Group will take into account:

- Any security incident reported via BCCG’s incident reporting system
- The results of the annual security audit

8. References

8.1 The following legislation and guidance has been taken into consideration in the development of this procedural document:

- The Private Security Industry Act 2001
- The Regulation of Investigatory Powers Act 2000
- Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013 (RIDDOR).
- Data Protection Act 1998
- The Protection from Harassment Act 1997
- Control of Substances Hazardous to Health 2002 Approved Codes of Practice (L5)
- The Health and Safety at Work Act 1974
- The Management of Health and Safety at Work Regulations 1999
- Human Rights Act 1998
- Criminal Procedure and Investigation Act 1996
- Police and Criminal Evidence Act 1984
- Criminal Justice and Public Order Act 1994
- CCTV Code of Practice 2000
- Standards for Commissioners 2015-16 NHS Protect.
- Equalities Act 2010

9. Review of the Policy

9.1 The policy will be approved by the Governing Body and reviewed at least every 2 years. The Health and Safety Group will monitor the policy on an ongoing basis. The procedural document will be reviewed every two years, and in accordance with the following on an as and when required basis:

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

Appendix 1

Definitions

1. **NHS Counter Fraud Authority**

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

   As a special health authority focused entirely on counter fraud work, the NHSCFA is independent from other NHS bodies and directly accountable to the Department of Health (DH).

2. **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.

3. **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 patient sit can also mean the personal possessions they retain whilst working in, using or providing services to the NHS.

4. **Premises**

   Premises are land and buildings together considered as a property.

Appendix 2

Reporting of Crime / Security Incidents

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

NHS Barnsley CCG Premises - Hillder 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 Competent Person for Security as soon as practicable.
- Completion of an Incident Reporting Form (as per Incident Policy) and a copy should be forwarded to the Competent Person for Security.

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.
- Completion of an Incident Report Form (as per Incident Policy) and a copy should be forwarded to the Competent Person for Security.

Out of Hours

- 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.

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. Close all windows and evacuate the room, lock all doors and leave the key in the lock. 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, 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 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.

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 and 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 3

NHS
Barnsley
Clinical Commissioning Group

Barnsley Clinical Commissioning Group

Lone Worker Procedure

Version:	1.0
Approved By:	Health & Safety Group
Date Approved:	October 2014, reviewed August 2017
Name of originator / author:	Ian Plummer, Ruth Nutbrown & Richard Walker
Name of responsible committee/ individual:	Health & Safety Group
Name of executive lead:	Richard Walker
Date issued:	October 2014, October 2018
Review Date:	3 years from approval
Target Audience:	All Barnsley CCG staff

LONE WORKER PROCEDURE

Amendment Log

Version No	Type of Change	Date	Description of change
V0.1	First Draft	September 2014	
V1.0	Final	October 2014	Finalised following H&S Group approval on 6.10.2014
V1.1	Review	August 2017	No changes

CONTENTS

BARNSLEY CLINICAL COMMISSIONING GROUP

LONE WORKER PROCEDURE

1. Introduction

1.1 This procedure sets out the steps the CCG will take to keep lone workers healthy and safe. The procedure has been developed in accordance with the CCG's Policy on the Development and Management of Policies and Procedures.

2. Purpose

2.1 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.

3. The risks of not having this procedure in place

3.1 In the absence of this procedure there is an increased risk that the CCG will not effectively discharge it's responsibility to address the health and safety risks for people working alone.

4. Definitions

4.1 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

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

5. Principles

5.1 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. Employers should take account of normal work and foreseeable emergencies, eg fire, equipment failure, illness and accidents. Employers should 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, eg 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?

6. Roles and Responsibilities

6.1 **The CCG** is responsible for the health, safety and welfare at work of all its workers 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.

6.2 **Line managers** are responsible for knowing the whereabouts of their staff; discussing potential risks to their staff arising from lone working; and putting in place appropriate, pragmatic actions to mitigate those risks (see procedure below).

6.3 **All staff** have responsibilities to take reasonable care of themselves and other people affected by their work activities and to co-operate with their employers in meeting their legal obligations.

7. Development, approval, and implementation

7.1 This procedure will be:

- Developed by the Head of Governance and Assurance with the support and expert input of the SY&BCCG's Health & Safety specialist
- Approved by the Health & Safety Group, which reports to the Audit Committee
- Disseminated to all CCG staff via email, staff bulletins, and the intranet.

8. Procedure

8.1 Staff working alone in Hillder House

8.1.1 Staff 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.

8.1.2 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.

8.1.3 Lone workers should always ensure they will be able to leave the office safely after working late. There have been instances where the building has been locked and people have been locked in.

8.2 Staff working alone at other locations

8.2.1 Lone workers must always ensure that 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.

8.2.2 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.

8.2.3 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.

8.3 **Lone working and vehicles**

8.3.1 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.

8.3.2 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.

8.3.3 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.

8.3.4 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.

8.4 **Escalation Procedure**

8.4.1 Line managers must discuss with their lone worker staff what actions they should take in the event of an incident.

8.4.2 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.

8.4.3 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.

8.4.4 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.

9. Monitoring the Compliance and Effectiveness of this Procedure

9.1 Compliance with, and effectiveness of, this procedure will be monitored by:

- Regular discussion and review by the Health & Safety Group
- Ongoing monitoring and review of incidents reported through the Safeguard incident reporting system.

10. References

10.1 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).

11. Review of the Procedure

11.1 The procedure will be reviewed at least every 2 years by the Health & Safety Group.

Appendix 4

NHS
Barnsley
Clinical Commissioning Group

Lone Worker Risk Assessment

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. Only one employee works on the premises, employees work separately from others and employees work outside normal hours

Area/Task: Lone working risk assessment for NHS Barnsley CCG staff

Date: August 2017 Persons Assessing the Risks: IP

Ref No:	***Activity/Task/ Area***	***Hazard Identified***	***Likelihood 1 – 5***	***Consequence 1 – 5***	***Risk Rating***	***Controls in place (including PPE as a last resort)***	***Recommended Additional Controls***	***Post Risk Rating***

Note: You should rate the risks on the basis of the current controls in place

1	Working outside normal office hours within Hillder house	There is a lone working risk of not receiving help in the event of an injury while working alone. Any injuries suffered could be exacerbated due to no first aide cover. This could result in litigation.	1	3	3 Low	Lone Worker procedure Mobile phone	Ensure lines of communication are available to lone workers who work outside office hours, line managers / colleagues are aware that the building is occupied, mobile phone numbers provided in the case of an emergency Lone worker to phone colleague when leaving the building at night.	3
2	Evening work within Hillder house	There is a risk of setting off the burglar alarm and not being able to reset it, which could result in the police visiting the site due to staff being locked in the	1	2	2	Lone Worker procedure	Ensure reception are aware that work is to be carried on after office hours, ensure the lone worker is aware of the procedure to set the alarm	2

		premises after hours.			Low	Mobile phone	Ensure that a manager / colleague is aware the person will be on site	
3	Working off site, within another building	There is a risk of staff being locked in with potentially no safe available means of escape due to late working at other sites, which could result in litigation.	1	2	2 Low	Meeting in diary, diary open to other staff Signing visitors sheets, Mobile phone	Advise staff to inform reception/ security that they plan to remain late if permitted. Ensure that a manager / colleague is aware the person will be on site	2
4	Travelling to and from meetings	There is a risk of injury to staff and others due to car incidents while travelling to and from other premises, which could result in litigation.	2	3	6 Med	Meetings in diary on outlook. Lone Worker Procedure. Mobile phone. Escalation procedure.	Conduct driving risk assessment and the development of a driving procedure. Be aware of your surroundings when driving, ensure your car is maintained and windows clean to aid visibility	3
5		There is a risk of injury due to Inclement weather while travelling to and from other premises, which could result in litigation.	2	3	6 Med		Check the weather forecast before travelling, if travel is required, it is advisable for warm clothes, food and a shovel is taken, ensure colleagues are aware, if there is an issue ensure your mobile phone is fully charged.	3
6	Walking from vehicle to meeting	There is a risk of injury due to slips, trips & falls while walking to or from a meeting, which could result in litigation.	2	2	4 Low	None	Ensure footwear is suitable when travelling. Always take your time, do not rush, park in well-lit areas were possible	2
7		There is a potential risk of physical / verbal aggression from members of the public while walking to or from a meeting, which could result in litigation and absence due to stress.	1	2	2 Low	None	Ensure personal items are not on show. Always park in well-lit areas were possible. Conflict resolution training could be delivered to front line staff	2
8		There is a risk of personal injury/suffering due to Inclement weather while walking to and from a meeting	1	2	2 Low	None	Check weather forecast before travelling, ensure clothing and footwear is suitable.	2
9		There is a risk of staff suffering from musculoskeletal issues from incorrect manual handling techniques due to carrying heavy bags for meetings which could result in long term illness and potential medical/legal costs to the business	1	3	3 Low	e-learning & practical manual handling training	Plan your meeting/journey ensure only work required is carried.	3

APPENDIX 5

Equality Impact Assessment

Title of policy or service:	Security Policy and Procedure	
Name and role of officer/s completing the assessment:	Richard Walker, Head of Assurance & Ruth Nutbrown, Assistant Chief Officer	
Date of assessment:	April 2015, Updated December 2017	
Type of EIA completed:	**Initial EIA 'Screening'** ☒ ***or*** **'Full' EIA process** ☐	*(select one option - see page 4 for guidance)*

1. Outline	
Give a brief summary of your policy or service	To protect staff, property and assets from a security threat. Produced in line with NHS Counter Fraud Authority guidance. The policy should be read alongside the CCG's Corporate Manual; Fraud, Bribery and Corruption Policy; Fire safety Policy; Health and Safety Policy; and Lone Worker Procedure.
What Outcomes do you want to achieve	
Give details of evidence, data or research used to inform the analysis of impact	
Give details of all consultation and engagement activities used to inform the analysis of impact	Ian Plummer, Health and Safety Manager, BCCG Health and Safety Group and Audit Committee.

Identifying impact:

- **Positive Impact:** will actively promote or improve equality of opportunity;
- **Neutral Impact:** where there are no notable consequences for any group;
- **Negative Impact:** negative or adverse impact causes disadvantage or exclusion. If such an impact is identified, the EIA should ensure, that as far as possible, it is either justified, eliminated, minimised or counter balanced by other measures. This may result in a ‘full’ EIA process.

2. Gathering of Information This is the core of the analysis; what information do you have that might *impact on protected groups, with consideration of the General Equality Duty*.					
	What key impact have you identified?			**For impact identified (either positive or negative) give details below:**	
(Please complete each area)	**Positive Impact**	**Neutral impact**	**Negative impact**	**How does this impact and what action, if any, do you need to take to address these issues?**	**What difference will this make?**
Human rights	☐	☒	☐		No anticipated detrimental impact has been identified on any equality group. The policy is applicable to all employees and adheres to NHSLA Standards, statutory requirements and best practice and makes all reasonable provision to ensure equity of access to all staff.
Age	☐	☒	☐		
Carers	☐	☒	☐		
Disability	☐	☒	☐		
Sex	☐	☒	☐		
Race	☐	☒	☐		
Religion or belief	☐	☒	☐		
Sexual orientation	☐	☒	☐		
Gender reassignment	☐	☒	☐		
Pregnancy and maternity	☐	☒	☐		
Marriage and civil partnership	☐	☒	☐		

(only eliminating discrimination)					
Other relevant groups	☐	☒	☐		
HR Policies only: Part or Fixed term staff	☐	☒	☐		

IMPORTANT NOTE: *If any of the above results in '**negative'** impact, a 'full' EIA which covers a more in depth analysis on areas/groups impacted must be considered and may need to be carried out.*

Having detailed the actions you need to take please transfer them onto the action plan below.

3. Action plan				
Issues/impact identified	**Actions required**	**How will you measure impact/progress**	**Timescale**	**Officer responsible**
No anticipated detrimental impact has been identified on any equality group. The policy is applicable to all employees and adheres to NHSLA Standards, statutory requirements and best practice and makes all reasonable provision to ensure equity of access to all staff.	There are no statements, conditions or requirements that disadvantage any particular group of people with a protected characteristic – therefore there is no required action identified.	The policy will be consulted on widely and will be monitored via the Equality and Diversity Steering Group/Management Team.		

4. Monitoring, Review and Publication				
When will the proposal be reviewed and by whom?	Lead / Reviewing Officer:	Head of Assurance	Date of next Review:	At time of Policy review

Once completed, this form **must** be emailed to the Equality Lead. barnsleyccg.equality@nhs.net

Equality Lead Signature: **Date: 12/01/2018**	Brigid Reid