NHS
Scarborough and Ryedale
Clinical Commissioning Group

SECURITY MANAGEMENT POLICY

Authorship :	Senior Internal Auditor
CCG Lead	Chief Finance Officer
Original Committee Approved :	Governing Body
Original Approval Date:	30 March 2016
Last Approval Committee	
Last Approval Date	
Review Date :	March 2019
Equality Impact Assessment :	Screening Completed
Sustainability Impact Assessment :	Completed
Target Audience :	All employees, members, committee and sub-committee members of the group and members of the governing body and its committees.
Policy Reference No. :	P400
Version Number :	V1

POLICY AMENDMENTS

Amendments to the Policy will be issued from time to time. A new amendment history will be issued with each change.

New Version Number	Issued by	Nature of Amendment	Approved by and Date	Date on Intranet

Contents

1 Policy Statement

1.1 Introduction

This policy covers the general security arrangements within the organisation and notes the relationship with other security related policies. In addition it covers the CCGs responsibilities as commissioners for ensuring that the services they commission are safe and secure.

1.2 Purpose, Aims and Objectives

The purpose of this policy is to detail NHS Scarborough and Ryedale CCG's responsibility for the effective management of security in relation to its corporate responsibilities for staff, patients, visitors and property and for its responsibilities as a commissioner for the security of commissioned services. The CCG is committed to the provision of safeguards against crime and the loss or damage to its own property and to the services its commissions.

To achieve this it is important for the CCG to:

- Develop a culture which recognises the importance of security;
- Provide and maintain a working environment that is safe and free from danger of crime for all people who may be affected by its activities including employees, patients/clients and visitors;
- Prevent loss of or damage to CCG assets and property as a result of crime, malicious acts, damage and trespass;
- Prescribe good order on premises under CCG control;
- Detect and report offenders to management and ensure a robust response in line with the national NHS Protect policies;
- Provide support for staff involved in a security incident, including incidents of violence and abuse, and supply up to date information for all parties especially after an incident;
- Comply with the NHS Protect Security Management Standards for Commissioners. The standards set out a framework for ensuring CCGs have proportionate security management arrangements within their organisation and also in ensuring that the services they commission are safe and secure.

1.3 Security Standards for Commissioners

The CCG will ensure it has arrangements in place to meet the requirements of the NHS Protect Security Management Standards for Commissioners. The CCG will determine its level of compliance through completion of a self-review tool (SRT). This is an annual requirement and will be returned to NHS Protect by the specified deadline. The SRT covers the key area of activity outlined in the standards and will be used to inform the development of an on-going review of the annual work plan by the LSMS in conjunction with the Executive Lead.

The policy covers specific responsibilities relating to:

- Corporate Security Management.
- Security Management in Provider Organisations.

2 Corporate Security Management

2.1 Purpose, Aims and Objectives

The CCG is committed to providing a safe place of work. To this end this policy is designed to introduce proactive procedures that will ensure, so far as reasonably practicable, not only the health and safety of its staff but the security of its buildings and resources.

This policy applies to staff employed by the CCG as well as contracted staff undertaking CCG duties, patients, visitors and others.

The central aim of this policy is to highlight the CCG's strategy in addressing the security and crime risks that confront the organisation with the objective of minimising potential losses through robust security control measures. This aim includes:

- The protection, safety, security and welfare of staff, patients, visitors, contractors and all who attend CCG premises;
- The provision of efficient and effective security control measures to minimise criminal activity including incidents of violence and aggression, loss, damage and/or theft of CCG property and assets;
- Minimising disruption to or loss of service to patients and staff.

The CCG strives to promote a pro-active security culture throughout the organisation. The CCG utilises a security and crime awareness approach, where staff are actively encouraged to support security and report all incidents and matters of concern as part of an effective security risk management process.

This process will ensure that adequate security measures are present through:

Ensuring that security surveys and risk assessments are carried out on the CCG premises and by departments to identify any security risks and recommend measures that are proportionate and commensurate with the risks highlighted, such measures may include:

- Unlocking and locking of premises
- Responding to violent, aggressive or abusive behaviour.
- Access to CCG premises including staff identification badges, key codes
- Lone working/ personal safety.
- Relevant arrangements for contractors to access premises as required;

- Ensuring adequate monitoring of such risk assessments to ensure compliance;
- Providing a secure environment for staff and all who interact with the organisation and, without prejudice to the interest of the organisation, their personal property;
- Liaison with the Police (both local and national levels), other relevant law enforcement and regulatory agencies (e.g. Environment Agency) and NHS Protect to identify security and crime risk trends;
- Providing support and assistance to staff, patients and visitors, as appropriate, who have been subject of a criminal act or exposed to an untoward security related incident.

2.2 Key Principles

In order to reduce crime, it is necessary to take a multi-faceted approach that is both proactive and reactive. The CCG has therefore adopted the three key principles designed to minimise the incidence of crime, and to deal effectively with those who commit crimes against the NHS:

- **Inform and Involve** those who work for or use the NHS about crime and how to tackle it. NHS staff and the public are informed and involved with a view to increase understanding of the impact of crime against the NHS.
- **Prevent and Deter** crime in the NHS to take away the opportunity for crime to occur or to re-occur and discourage those individuals who may be tempted to commit crime, by implementing robust systems, which will be put in place in line with policy, standards and guidance developed by NHS Protect. Successes may be publicised so that the risk and consequences of detection are clear to potential offenders.
- **Hold to Account** those who have committed crime against the NHS. Crimes must be detected and investigated, suspects prosecuted where appropriate, and redress sought where possible. Where necessary and appropriate, this work will be conducted in partnership with the police and other crime prevention agencies. Where recovery of monies lost to crime is viable, this will be pursued. In relation to crimes against NHS staff, criminal damage or theft against NHS property, investigation and prosecution will be undertaken in liaison with the police and CPS or where necessary NHS Protect.

3 Roles and responsibilities for Corporate Security Management

3.1 Accountable Officer

The Accountable Officer has responsibility to ensure that systems are in place to ensure that the risk to employees is minimised as far as reasonably practicable.

3.2 Executive Lead

The Chief Finance Officer has been designated as the Executive Lead to take responsibility for security management matters.

The Executive Lead, on behalf of the Accountable Officer, is responsible for ensuring that the CCG's Security Policy is implemented within the organisation.

This will include the responsibility for:

- Assisting the Local Security Management Specialist in the performance of their duties, including the investigation of incidents, security assessment of working areas and the reporting of all security related incidents;
- 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 that adequate funding is allocated for necessary security measures within the CCG premises. They should also ensure that security implications are considered as part of tendering processes for new and existing services.

Reports on Security management and any incidents will be reported to the Audit and Governance Committee.

3.3 Local Security Management Specialist (LSMS)

The CCG is required to nominate an individual as the Local Security Management Specialist (LSMS). NHS Protect are to be informed of any such nomination. The nominated individual must be trained by NHS Protect to undertake the LSMS role. The LSMS will:

- Report directly to the Executive Lead and be responsible for liaising between the CCG and NHS Protect;
- Report to NHS Protect any weaknesses in security related systems of the NHS body or other matters which the LSMS considers may have implications for security management in the NHS;
- Prepare a written work plan, with the Executive Lead and prepare regular reports on progress against that plan to the Audit and Governance Committee;
- Provide competent advice on the CCGs management of security;
- Review security policies;
- Conduct security risk assessments; (and include/escalate risks to the risk register in line with the CCG's risk management strategy);
- Review security incidents and report all incidents of violence and aggression, as required, to the police where appropriate and NHS Protect;
- Identify learning from security incidents and review policies and procedures to prevent reoccurrence;

- Attend the relevant committees; and provide progress and annual reports;
- Monitor progress made against recommendations arising from security audits;
- Assist local managers in carrying out investigations into security related incidents, liaising as required with local Police, the Criminal Justice Unit and the Legal Protection Unit and where necessary preparing case files for submission to Court as part of the prosecution process;
- To foster links with local agencies and bodies, such as Police, Crime and Disorder Reduction Partnerships and other security professionals in neighbouring NHS organisations;
- Ensuring completion of self-assessment tool for review by the Executive Lead.

3.4 Managers

Managers are responsible for:

- Their own teams' security in terms of providing a safe and secure environment;
- Ensuring their staff understand and comply with this policy;
- Ensuring all significant security risks are identified and measures are implemented to establish a safe and secure environment;
- Actively encouraging the reporting of incidents relating to security issues in accordance with the CCG's incident reporting procedures;
- The initial investigation of any incident related to a security issue and/or violence at work, involving the LSMS at an appropriate stage.

3.5 Employee's Responsibilities

Employees should:

- Familiarise themselves with the content of this policy and associated procedures;
- Familiarise themselves with any special security requirements relating to their place of work;
- Safeguard themselves, colleagues, visitors, clients etc., so far as is reasonably practicable;
- Ensure that neither equipment nor properties are put in jeopardy by their actions, either by instruction, example or behaviour;
- Co-operate in the completion of risk assessments;
- Comply with policies/procedures, control measures and safe systems of work;
- Report any security concerns/breaches or incidents as soon as possible;
- Attend appropriate training sessions;
- Provide support and co-operation with any investigations;
- Use all security equipment in accordance with any training and instructions given e.g. panic alarms;

- Remain alert to the presence of unusual and unexplained packages, which cannot readily be identified. Any such package should be reported immediately to a supervisor or line manager. Under no circumstances should a suspect package be handled.
- Wear CCG identity badges at all times unless otherwise directed due to control of infection or personal safety.

4 Risk Management Strategy

4.1 Risk Management

Risk Management is at the heart of the Security Strategy. Risk management techniques harness the information and experience of CCG staff (and external expertise if necessary); translating this into positive action to remove or manage hazards and reduce risks.

4.2 Risk Assessment

A security risk assessment will need to be completed and reflected in the risk register. The risks should be reflected in an annual work plan along with clear objectives that are measurable. The plan will be monitored by the Executive Lead to ensure that resources to mitigate the risks are sufficient).

Security risk assessment involves:

- Review of the various activities of the CCG and identification of critical areas for the organisation;
- Identification of the risks that exist:
    - What could go wrong?
    - How could it happen?
    - What would be the effect?
- Assessing those risks for potential frequency and severity;
- Eliminating the risks that can be eliminated;
- Identifying how remaining risks can be mitigated or managed;
- Developing and delivering a plan for implementing the identified changes;
- Provides current measurement and assists target setting for reduction in risks.

The CCG will carry out appropriate risk scoping on physical security of premises and assets every year. Where properties are leased, the risk assessment may be undertaken in conjunction with the owners of the premises occupied by the CCG. Following a risk assessment on premises or assets an action plan will be developed with timescales and nominated persons to carry out agreed action. Relevant policies will be revised or developed where required to address risks identified through the risk assessment process. Such policies will be monitored for effectiveness via meaningful data and kept under

review for changes where required. Policies will be communicated across the organisation.

If new premises or assets are commissioned within the CCG these will be risk assessed prior to operational use of them, in line with this policy.

A security assessment check sheet is included at Appendix A of this policy.

5 Security-specific risk management measures

5.1 CCG Premises

Following risk assessment, managers are responsible for developing any local procedures required to ensure security of premises, for example, arrangements for the items listed below. This list is not exhaustive and managers may identify other issues:

- Unlocking and locking of premises;
- Responding to violent, aggressive or abusive behaviour;
- Access to CCG premises including staff identification badges, access controls;
- Lone working/personal safety;
- Relevant arrangements for contractors to access premises as required.

5.2 Premises Access Controls to be added specific to each CCG

Access to CCG premises is by security controlled entrances. The main CCG offices are controlled by computer controlled key fobs, with authorisation required for issue of the fobs. Access to Sovereign House is by a manual key pad, with the code restricted, and changed regularly.

5.3 Identification Badges

ID badges are issued to all staff on commencement of employment. ID badges must be worn at all times whilst on CCG premises or business. Persons not wearing an ID badge should be challenged and asked to identify themselves.

When staff leave CCG employment, all ID badges should be returned to the Manager and destroyed. If an ID badge is lost or stolen this must be reported to the Manager and reported via the CCG incident reporting system.

5.4 Visitors / Contractors

All visitors / contractors are to be signed in and out of CCG premises. For security reasons all visitors must be escorted to and from their destination within CCG buildings.

5.5 CCG Property / Assets

Managers are responsible for undertaking risk assessments regarding the security of assets held within their departments and this should be included in the service / departmental general risk assessment. Where appropriate, items should be placed on the asset register or an appropriate inventory depending on value. Managers should review CCG property held by their department on a regular basis to ensure that all items are securely managed.

All managers and staff should take all reasonable steps to safeguard CCG property whilst it is in their care. Members of staff should not remove property belonging to the CCG without prior authority from their line manager or the custodian of the equipment. Failure to obtain authority could result in disciplinary action or criminal proceedings being taken.

5.6 Personal Property

Staff should be aware that the CCG cannot accept liability for loss or damage to staff property brought onto its premises.

Staff are advised to take adequate precautions to ensure the safety of their possessions and not bring valuables to work. Where storage has been provided for personal use, the individual to whom it is allocated will be responsible for ensuring it is locked.

Staff must report any loss of, or damage to, their belongings and co-operate in any consequent inquiry into the loss or damage. If private property has been stolen then it is the owners and not the CCGs responsibility to report the matter to the Police. This should be after notifying a line manager and reporting the incident. Any reference number assigned should also be recorded in the incident log.

5.7 Security of Motor Vehicles

The CCG cannot accept liability for any private motor vehicle or its contents when they are parked on a CCG site or when the car is being used by an employee on CCG business.

5.8 Lease Cars

In the event of an incident or accident involving a lease car, the employee must notify their manager and the lease car management company in accordance with the lease car policy issued to them.

5.9 Prevention of Violence to Staff

The CCG has a duty to provide a safe and secure environment for all employees and visitors and has a zero tolerance approach to violence or abusive behaviour. The CCG takes a very serious view of violence, abuse and aggression at work and recognises its responsibility to protect employees and others who may be subjected to any acts of violence, abuse or aggression

whether or not the act results in physical or non-physical assault and whether carried out by members of the public, patients, relatives or by members of staff. Violent or abusive behaviour will not be tolerated and decisive action will be taken by the CCG to protect staff, patients and visitors.

5.10 Bomb Threats and the Law

The CCG should be vigilant to situations where bomb threats are received. Making such malicious calls is an offence contrary to Section 51 of the Criminal Law Act and should always be reported to the police. Any member of staff receiving such a call should seek the immediate advice of the most senior manager available.

5.11 Personal Safety and Lone Working

Managers must ensure that a risk assessment is undertaken and documented, for all staff considered to be lone workers. The risk assessment should include precautions to reduce the likelihood of harm occurring.

The CCGs Lone Working Policy must be referred to and complied with.

5.12 Information Security

All staff must abide by the code of confidentiality issued by the CCG which seeks to ensure all information matters relating to the organisation, their employment, other members of staff and the general public comply with the Caldicott Principles and Government legislation, for example:

- Data Protection Act 1998;
- The Computer Misuse Act 1990;
- Copyrights and Patents Act 1998;
- The Human Rights Act 1998.

There is a suite of Information Governance policies available which must be referred to within the NHS Scarborough and Ryedale CCG. Please familiarise yourself with these.

6 Security incident reporting

6.1 Incident Reporting

All security related incidents / near misses should be reported to local line management and the LSMS, using the CCG incident form, if urgent but not criminal. A local investigation should be initiated by managers.

All incidents of crime should be reported to the local Police Station. The LSMS should be notified as soon as possible by telephone / email and by the completion of a CCG reporting form.

Examples of reportable incidents include, but are not limited to:

- Physical assault or verbal abuse by a patient, visitor or another member of staff towards a member of staff;
- Physical assault or verbal abuse by a member of staff towards a patient or visitor;
- Any incident which is racially or religiously aggravated
- Theft of staff or CCG property;
- Damage to premises that was the result of criminal activity (including arson)

If you are in any doubt as to what is reportable and what isn't, you should contact the LSMS.

6.2 Assisting the Police with Investigations

From time to time the police may contact the CCG for information relating to an on-going investigation. An individual who is contacted in such a manner should refer the Police to the LSMS or the Executive Lead.

Staff should obtain guidance from Information Governance on when and the extent of confidential information may be disclosed.

6.3 Learning from Incidents

The CCG will ensure that learning from incidents is reviewed and leads to policy and procedural changes to prevent reoccurrence. This will be incorporated in the workplan of the LSMS.

7 Assuring Security Management in Provider Organisations

7.1 Introduction

Under the NHS Standard Contract all organisations providing NHS services (providers) must put in place and maintain appropriate anti-crime arrangements. The NHS organisations which commission the services (commissioners) should review providers' arrangements to make sure they meet the requirements under the contract.

As a commissioning organisation, the CCG has responsibilities under the NHS Protect Security Standards for Commissioners for ensuring that the services they commission are safe and secure.

The primary areas of activity to be undertaken by the CCG will be to ensure providers of commissioned services comply with the current security standards for providers.

8 Roles and Responsibilities for Assuring Security Management in Provider Organisations

8.1 Accountable Officer

The Accountable Officer has responsibility to ensure that systems are in place for the organisation to obtain assurance on the security management arrangements in provider organisations.

8.2 Executive Leads

The Chief Finance Officer has been designated as the Executive Lead to take responsibility for security management matters.

8.3 Local Security Management Specialist (LSMS)

- To provide guidance and support to the organisation on seeking assurance from provider organisations where required.
- To provide guidance and support to the organisation when reviewing findings from the investigation of serious incidents at provider organisations.

8.4 Contracting Team

- Where the organisation is the commissioner or lead commissioner seek assurance (in accordance with Service Condition 24 of the NHS Standard Contract) that the NHS Provider meets the requirements of the standard commissioning contract; including the completion of a NHS Protect issued Self Review Tool (SRT) in respect of Security Management if they are Monitor licensed or a Trust~~including completion of an organisation crime profile and implementation of NHS Protect standards for providers.~~
- Use the NHS Standard Contract when commissioning NHS funded services.

9 Security awareness measures

9.1 Training

Managers will determine the level of training required by their staff and reassess this training need as and when their roles / job changes.

Staff will be provided with access to the policy, and a brief overview of relevant areas, as part of their local induction. Staff will be expected to read the policy as part of their induction process.

Health and Safety training is a statutory requirement of legislation and therefore mandatory for all staff of the CCG (aspects of security training cut across health and safety training). A range of training will be available to staff through e-learning.

All new permanent employees must complete mandatory training at the earliest practicable time after commencing employment. This training includes Health and Safety, Fire, Information Governance and Manual Handling.

Managers are to identify any specific security related training needs for the staff they are directly responsible for and must make adequate arrangements for staff to be able to attend.

9.2 Dissemination and Implementation of policy

The CCG will ensure that a copy of this policy is freely available to all CCG staff (electronically and/or hard copy). Managers should receive the appropriate advice to ensure the content of this policy is fully implemented

10 Monitoring of policy effectiveness

10.1 Monitoring

Managers will be responsible for monitoring and reviewing their own local security risk assessments and associated building arrangements. The review of policies will also be based on the prioritisation of risk within the CCG and as a consequence of any serious incidents.

The LSMS reviews all risk assessments and all incidents relating to security of premises and assets and reports to relevant staff and committees as soon as practicable after the event;

- Risk assessments:
    - Trends
    - Progress with action plans
    - Blocks to implementation
- Incidents
    - Number
    - Trends
    - Progress with action plans
    - Blocks to implementation

Security breaches and other loss events will be reported on a regular basis to the Audit and Governance Committee. The investigation of such incidents will be used as a tool to identify common causes, assist police, prevent reoccurrence and assess the effectiveness of policy controls.

Breaches of this policy may be investigated and may result in the matter being treated as a disciplinary offence under the CCGs disciplinary procedure.

10.2 Reporting

To provide assurance on the effectiveness of the policy, the LSMS will report directly to the Executive Lead and attend the Audit and Governance Committee to provide progress and annual reports.

11 Related policies

Associated documents and policies:

- Anti-fraud & Bribery policy
- Incident reporting policy
- Whistleblowing policy
- Standards of business conduct
- Zero tolerance policy
- Lone workers policy
- Lock down procedures
- Emergency planning
- Business continuity
- Risk management strategy / policy
- Information security policy

12 References and Definitions

12.1 References

- Health and Safety at Work Act 1974
- Management of Health and Safety at Work Regulations 1999
- NHS Standard Contract (National Commissioning Contract)
- Crime and Disorder Act 1998
- Data Protection Act 1998
- Workplace Health, Safety and Welfare Regulations 1992
- Freedom of Information Act 2000
- Human Rights Act 1998 (in particular article 8 ‘Human Rights Bill 1998 – the right to respect for private and family life’)
- NHS Protect Standards for Commissioners – Security Management

12.2 Definitions

- NHS Protect: This organisation has responsibility for all policy and operational matters relating to the prevention, detection and investigation of fraud and corruption and the management of security in the National Health Service.
- Physical Security: This term as understood by Health and Safety professionals relates to buildings and objects as any security hardware

including locks, access control, intruder alarms, panic alarms, barriers etc that supports the security function.

- Security: A state of being where the risks to people and property are minimised in relation to any actions that may lead to personal injury, threat to life or the disruption of business activity of the organisation.
- Security Incident: Any act or omission that has the potential to undermine the integrity of the CCGs security objectives and would include non-compliance whether deliberate or otherwise with the CCG Security Policy and/or local security arrangements.
- Criminal Act: Any violation or attempted violation of law whether statute or common law and would include such offences that are more likely to occur within the healthcare setting such as:
    - Harassment;
    - Assaults and threats of violence;
    - Theft and kindred offences such as burglary;
    - Criminal damage;
    - Offences relating to public disorder;
    - Fraud.
- Premises: The physical buildings, grounds and all property contained within the CCG boundaries in which NHS staff and professionals work and from which the business of the NHS is delivered.
- Assets: Irrespective of their value, ‘Assets’ can be defined as the materials and equipment used directly or indirectly to deliver NHS healthcare. In respect of staff, professionals and patients, the definition can also apply to their personal possessions they retain whilst on CCG premises or working in or providing a service to the NHS.

13 Security Risk Assessment Check Sheet

Name of organisation:	
Address of premise:	
Identification of area within the premise:	
Date of Assessment:	
Assessment undertaken by (print name):	

Security Management					
	Yes/No	**Risk Level Low / Med / High**	**Rationale for risk assessment**	**Required action**	**Target Date/ Complete**
1 Has a suitable and sufficient workplace security risk assessment been carried out identifying all significant hazards?					
2 Is the security risk assessment readily available and does it identify control measures to either remove or reduce hazards?					
3 Are risks placed on the Risk Register updated or removed as appropriate?					
4 Have management developed safe systems of work for work activities to protect persons within the premise?					

Security Management					
	Yes/No	**Risk Level Low / Med / High**	**Rationale for risk assessment**	**Required action**	**Target Date/ Complete**
5 Are staff aware of organisational security procedures and suitable trained?					
6 Does the work place have an effective security alarm system?					
7 Is there suitable monitoring of security measures in place?					
8 Are security arrangements regularly monitored?					
9 Is the workplace risk assessment regularly/annually reviewed?					
Security Prevention – General					
	Yes/No	**Risk Level Low / Med / High**	**Rationale for risk assessment**	**Required action**	**Target Date/ Complete**
10 Is there an effective system for ensuring that access to the premise is suitably secure and persons within the premise are readily identifiable?					
11 Is there an effective procedure/system for ensuring external/internal accommodation is secured when un-occupied?					

Security Management					
	Yes/No	**Risk Level Low / Med / High**	**Rationale for risk assessment**	**Required action**	**Target Date/ Complete**
12 Is there an effective system for the recording of organisational assets and equipment within the workplace?					
13 Are all employees provided with and display photographic/name identification?					
14 Are all employees in high risk areas properly informed of the particular risks and the means to control the risks?					
15 Is external lighting (where provided) suitable to illuminate persons wishing to gain entry to the premise?					
16 Are all security related incidents recorded and reported in accordance with CCG Risk Management Policy using the Incident Reporting Form?					

Security Prevention – Employees					
	Yes/No	**Risk Level Low / Med / High**	**Rationale for risk assessment**	**Required action**	**Target Date/ Complete**
17 Has a security training needs analysis been completed for staff within the workplace (i.e. Personal Safety Plan)?					
18 Are training records readily available?					
19 Has a Lone Worker Assessment been undertaken and control measures identified implemented?					
20 Are staff made aware that the CCG will not accept liability for the loss of personal belongings within the workplace?					

Security – Access					
	Yes/No	**Risk Level Low / Med / High**	**Rationale for risk assessment**	**Required action**	**Target Date/ Complete**
21 Is there an effective procedure for the registration security, monitoring and distribution of keys?					
22 Are keys issued against a name, date, and signature?					
23 Are distributed keys checked on a regular basis by management?					
24 Are security codes for doors fitted with digital access recorded and changed regularly or on change of staff?					
25 Are suitable procedures available for staff to challenge unidentified persons or persons in unauthorised area within the premise?					
26 Is there an effective procedure for recording all persons within the workplace?					

Security - Confidential Information					
	Yes/No	**Risk Level Low / Med / High**	**Rationale for risk assessment**	**Required action**	**Target Date/ Complete**
27 Are adequate arrangements in place for compliance with CCG Policies and Procedures on Confidentiality of Information for: ○ Patient Medical Records ○ Employee Personnel Records ○ Complaints ○ Financial ○ Contracts for Services and Goods					
28 Is all data information contained on electronic retrieval systems securely protected in accordance with CCG Policy?					

Security Assessment Check Sheet Results

If all answers to the questions above are 'Yes' or 'N/A', security arrangements are considered to be adequate; no further action is required at this time. Simply sign and date the form in the space provided below.

If one or more answers to the questions above are 'No', your security arrangements may be considered inadequate and needs to be addressed if applicable to the workplace.

APPENDIX B: SUSTAINABILITY IMPACT ASSESSMENT

Staff preparing a policy, Governing Body (or Sub-Committee) report, service development or project are required to complete a Sustainability Impact Assessment (SIA). The purpose of this SIA is to record any positive or negative impacts that this is likely to have on sustainability.

Title of the document	Security Management Policy
What is the main purpose of the document	
Date completed	November 2015
Completed by	Richard Mellor

Domain	**Objectives**	**Impact of activity** Negative = -1 Neutral = 0 Positive = 1 Unknown = ? Not applicable = n/a	**Brief description of impact**	**If negative, how can it be mitigated? If positive, how can it be enhanced?**
Travel	Will it provide / improve / promote alternatives to car based transport? Will it support more efficient use of cars (car sharing, low emission vehicles, environmentally friendly fuels and technologies)? Will it reduce 'care miles' (telecare, care closer) to home? Will it promote active travel (cycling, walking)? Will it improve access to opportunities and facilities for all groups?	0		
Procurement	Will it specify social, economic and environmental outcomes to be accounted for in procurement and delivery? Will it stimulate innovation among providers of services related to the delivery of the organisations' social, economic and environmental objectives? Will it promote ethical purchasing of goods or services? Will it promote greater efficiency of resource use? Will it obtain maximum value	0		

	from pharmaceuticals and technologies (medicines management, prescribing, and supply chain)? Will it support local or regional supply chains? Will it promote access to local services (care closer to home)? Will it make current activities more efficient or alter service delivery models			
Facilities Management	Will it reduce the amount of waste produced or increase the amount of waste recycled? Will it reduce water consumption?	0		
Workforce	Will it provide employment opportunities for local people? Will it promote or support equal employment opportunities? Will it promote healthy working lives (including health and safety at work, work-life/home-life balance and family friendly policies)? Will it offer employment opportunities to disadvantaged groups?	0		
Community Engagement	Will it promote health and sustainable development? Have you sought the views of our communities in relation to the impact on sustainable development for this activity?	0		
Buildings	Will it improve the resource efficiency of new or refurbished buildings (water, energy, density, use of existing buildings, designing for a longer lifespan)? Will it increase safety and security in new buildings and developments? Will it reduce greenhouse gas emissions from transport (choice of mode of transport, reducing need to travel)? Will it provide sympathetic and appropriate landscaping around new development? Will it improve access to the built environment?	1		

Adaptation to Climate Change	Will it support the plan for the likely effects of climate change (e.g. identifying vulnerable groups; contingency planning for flood, heat wave and other weather extremes)?	0		
Models of Care	Will it minimising 'care miles' making better use of new technologies such as telecare and telehealth, delivering care in settings closer to people's homes? Will it promote prevention and self-management? Will it provide evidence-based, personalised care that achieves the best possible outcomes with the resources available? Will it deliver integrated care, that co-ordinate different elements of care more effectively and remove duplication and redundancy from care pathways?	0		

APPENDIX C: EQUALITY IMPACT ANALYSIS

1. Equality Impact Analysis	
Policy / Project / Function:	Security Management Policy
Date of Analysis:	November 2015
This Equality Impact Analysis was completed by: (Name and Department)	Richard Mellor, Finance
What are the aims and intended effects of this policy, project or function?	Security management
Please list any other policies that are related to or referred to as part of this analysis	
Who does the policy, project or function affect? Please Tick ✓	Employees ✓ Service Users ✓ Members of the Public ✓ Other (List Below)

2. Equality Impact Analysis: Screening					
	Could this policy have a positive impact on…		Could this policy have a negative impact on…		Is there any evidence which already exists from previous (e.g. from previous engagement) to evidence this impact.
	Yes	No	Yes	No	
Race		X		X	
Age		X		X	
Sexual Orientation		X		X	
Disabled People		X		X	
Gender		X		X	
Transgender People		X		X	
Pregnancy and Maternity		X		X	
Marital Status		X		X	
Religion and Belief		X		X	
Reasoning	The policy looks to protect all staff and visitors to CCG premises. There is no difference in application due to any of the protected characteristics				
If there is no positive or negative impact on any of the Nine Protected Characteristics go to Section 7.					

3. Equality Impact Analysis: Local Profile Data	
Local Profile/Demography of the Groups affected (population figures)	
General	
Age	
Race	
Sex	
Gender reassignment	
Disability	
Sexual Orientation	
Religion, faith and belief	
Marriage and civil partnership	
Pregnancy and maternity	

4. Equality Impact Analysis: Equality Data Available	
Is any Equality Data available relating to the use or implementation of this policy, project or function? Equality data is internal or external information that may indicate how the activity being analysed can affect different groups of people who share the nine Protected Characteristics – referred to hereafter as 'Equality Groups'. Examples of Equality data include: (this list is not definitive) 1. Application success rates Equality Groups 2. Complaints by Equality Groups 3. Service usage and withdrawal of services by Equality Groups 4. Grievances or decisions upheld and dismissed by Equality Groups 5. Previous EIAs	Yes No Where you have answered yes, please incorporate this data when performing the Equality Impact Assessment Test (the next section of this document).
List any Consultation e.g. with employees, service users, Unions or members of the public that has taken place in the development or implementation of this policy, project or function.	
Promoting Inclusivity **How does the project, service or function contribute towards our aims of eliminating discrimination and promoting equality and diversity within our organisation.**	

5. Equality Impact Analysis: Assessment Test				
What impact will the implementation of this policy, project or function have on employees, service users, or other people who share characteristics protected by The Equality Act 2010?				
Protected Characteristic:	**No Impact:**	**Positive Impact:**	**Negative Impact:**	**Evidence of impact and if applicable, justification where a Genuine Determining Reason exists**
Gender (Men and Women)				
Race (All Racial Groups)				
Disability (Mental and Physical)				
Religion or Belief				
Sexual Orientation (Heterosexual, Homosexual and Bisexual)				
Pregnancy and Maternity				
Transgender				
Marital Status				
Age				

6. Action Planning				
As a result of performing this analysis, what actions are proposed to remove or reduce any risks of adverse outcomes identified on employees, service users or other people who share characteristics protected by The Equality Act 2010?				
Identified Risk:	**Recommended Actions:**	**Responsible Lead:**	**Completion Date:**	**Review Date:**

7. Equality Impact Analysis Findings				
Analysis Rating:	Red	Red/Amber	Amber	Green
		Actions	**Wording for Policy/Policy/Function**	
Red **Stop and remove the policy**	As a result of performing the analysis, it is evident that a risk of discrimination exists (direct, indirect, unintentional or otherwise) to one or more of the nine groups of people who share Protected Characteristics. It is recommended that the use of the policy be suspended until further work or analysis is performed.	**Remove the policy** Complete the action plan above to identify the areas of discrimination and the work or actions which needs to be carried out to minimise the risk of discrimination.	No wording needed as policy is being removed.	
Red Amber **Continue the policy**	AS a result of performing the analysis, it is evident that a risk of discrimination exists (direct, indirect, unintentional or otherwise) to one or more of the nine groups of people who share Protected Characteristics. However, a genuine determining reason may exist that could legitimise or justify the use of this policy and further professional advice should be taken.	**The policy can be published with the EIA** List the justification of the discrimination and source the evidence (i.e. clinical need as advised by NICE). Consider if there are any potential actions which would reduce the risk of discrimination. Another EIA must be completed if the policy is changed, reviewed or if further discrimination is identified at a later date.	As a result of performing the analysis, it is evident that a risk of discrimination exists (direct, indirect, unintentional or otherwise) to one or more of the nine groups of people who share Protected Characteristics. However, a genuine determining reason exists which justifies the use of this policy and further professional advice. ***[Insert what the discrimination is and the justification of the discrimination plus any actions which could help what reduce the risk]***	
Amber **Adjust the Policy**	As a result of performing the analysis, it is evident that a risk of discrimination (as described above) exists and this risk may be removed or reduced by implementing the	**The policy can be published with the EIA** The policy can still be published but the Action Plan must be monitored to	As a result of performing the analysis, it is evident that a risk of discrimination (as described above) exists and this risk may be removed or reduced by implementing the actions detailed within the Action Planning section of this document. ***[Insert what the discrimination is and what work will be***	

	actions detailed within the Action Planning section of this document.	ensure that work is being carried out to remove or reduce the discrimination. Any changes identified and made to the service/policy/strategy etc. should be included in the policy. Another EIA must be completed if the policy is changed, reviewed or if further discrimination is identified at a later date.	***carried out to reduce/eliminate the risk]***
Green **No major change**	As a result of performing the analysis, the policy, project or function does not appear to have any adverse effects on people who share Protected Characteristics and no further actions are recommended at this stage.	**The policy can be published with the EIA** Another EIA must be completed if the policy is changed, reviewed or if any discrimination is identified at a later date.	As a result of performing the analysis, the policy, project or function does not appear to have any adverse effects on people who share Protected Characteristics and no further actions are recommended at this stage.

Brief Summary/Further Comments	

Approved By		
Job Title:	Name:	Date: