Creating a
healthier
Hull

NHS
Hull
Clinical Commissioning Group

SECURITY MANAGEMENT POLICY

DECEMBER 2018

Important: This document can only be considered valid when viewed on the CCG's website.

If this document has been printed or saved to another location, you must check that the version number on your copy matches that of the document online.

Name of Policy:	Security Management Policy
Date Issued:	January 2019
Date to be reviewed:	December 2020 (and two years thereafter or of statutory changes required)

Policy Title:	Security Management Policy	
Supersedes: (Please List)	Security Management Policy (July 2016)	
Description of Amendment(s):	Updated Policy in line with the demise of NHS Protect and introduction of new legislation.	
This policy will impact on:	All CCG employees on permanent or temporary contracts (including Board Members) & bank and Agency Staff volunteers & visitors	
Policy Area:	Finance	
Version No:	2.1	
Author:	Gary Ross Local Security Management Specialist	
Effective Date:	January 2019	
Review Date:	December 2020	
Equality Impact Assessment Date:	December 2018	
APPROVAL RECORD		**Date:**
	Health, Safety and Security Meeting	25.01.19
	Integrated Audit and Governance Committee	28.01.19
Consultation:	Health, Safety and Security Meeting	23.04.18
	Senior Leadership Team	23.04.18

CONTENTS

1. INTRODUCTION

Hull Clinical Commissioning Group (hereafter referred to as ‘CCG’) has a duty of care to ensure high quality health services are provided in a safe and secure environment which protects staff, patients, service users, and stakeholders. This policy sets out processes of how Hull CCG assesses security risks, manages any actions arising from this analysis and how security incidents are reported and managed.

It has been produced in order to ensure that the CCG meets all of its UK Legislative (both Statute and Common Law) obligations as well as regulatory and contractual requirements.

This would encompass those requirements necessary to protect the health, safety and welfare of its staff, service users and stakeholders, from criminal activity, violence aggression and abuse, as well as general security management matters.

The policy covers the security management arrangements within the organisation and notes the relationship with other security related policies and officers/agencies.

2. SCOPE

This policy and guidance is applicable without exception to all staff working within NHS Hull CCG, whether directly, or indirectly, employed.

3. POLICY PURPOSE AND AIMS

The purpose and aims of this policy are to detail NHS Hull CCG’s responsibility for the effective management of security in relation to staff, visitors and property. The CCG is committed to the provision of safeguards against crime and the loss or damage to its property and/or equipment. 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, via the appropriate incident reporting system in use within the CCG and ensure a robust response in line with its statutory and common law obligations;
- Provide support for staff involved in a security incident and supply up to date information for all parties especially after an incident;
- Continually improve performance with regard to security through the participation, commitment and support of other organisation and of all staff to ensure security of its premised, staff, patients and visitors.

4. IMPACT ANALYSIS

4.1 Equality

All policies require an assessment for their impact on people with protected characteristics. An Equality Impact Assessment has been undertaken for this policy and as a result of performing the analysis, it is evident that there is no risk of discrimination in the implementation of this policy. The assessment can be found in Appendix A.

.

The CCG is committed to applying this policy, the CCG will have due regard for the need to eliminate unlawful discrimination, promote equality of opportunity, and provide for good relations between people of diverse groups, in particular on the grounds of the following characteristics protected by the Equality Act (2010); age, disability, gender, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, and sexual orientation, in addition to offending background, trade union membership, or any other personal characteristic.

4.2 Statutory Provision

NHS Hull Clinical Commissioning Group has a responsibility to ensure that all staff are made aware and cognizant with their duties and responsibilities arising from any/all Statutory and Common Law provisions applicable to ensuring both their, and their colleagues, safety, security and wellbeing.

If you require assistance in determining the range, nature or implications of the above please contact the Local Security Management Specialist on telephone number 07906 651391 or email at gary.ross@audit-one.co.uk,

Due consideration has been given to the appropriate criminal/civil law requirements in the development of this policy document and no specific risks were identified.

5. NHS CONSTITUTION

5.1 The CCG is committed to:

- **Working together for patients** – Patients come first in everything we do. We fully involve patients, staff, families, carers, communities, and professionals inside and outside the NHS. We put the needs of patients and communities before organisational boundaries. We speak up when things go wrong.

- **Respect and Dignity** – We value every person – whether patient, their families or carers, or staff – as an individual, respect their aspirations and commitments in life, and seek to understand their priorities, needs, abilities and limits. We take what others have to say seriously. We are honest and open about our point of view and what we can and cannot do.

- **Commitment to quality of Care** – We earn the trust placed in us by insisting on quality and striving to get the basics of quality of care – safety, 12 effectiveness and patient experience – right every time. We encourage and welcome feedback from patients, families, carers, staff and the public. We use this to improve the care we provide and build on our successes

- **Compassion** – We ensure that compassion is central to the care we provide and respond with humanity and kindness to each person’s pain, distress, anxiety or need. We search for the things we can do, however small, to give comfort and relieve suffering. We find time for patients, their families and carers, as well as those we work alongside. We do not wait to be asked, because we care.

- **Improving lives** – We strive to improve health and wellbeing and people’s experiences of the NHS. We cherish excellence and professionalism wherever we find it – in the everyday things that make people’s lives better as much as in clinical practice, service improvements and innovation. We recognise that all have a part to play in making ourselves, patients and our communities healthier.

- **Everyone counts** – We maximise our resources for the benefit of the whole community, and make sure nobody is excluded, discriminated against or left behind. We accept that some people need more help, that difficult decisions have to be taken – and that when we waste resources we waste opportunities for others.

5.2 This Policy supports the NHS Constitution and its obligations and mandatory and statutory requirements.

6. ROLES/RESPONSIBILITIES/DUTIES

6.1 Accountable Officer

The Accountable Officer has overall responsibility on behalf of the CCG Governing Body and is responsible for the organisation and management of security management measures across the CCG and monitoring of the implementation of this policy throughout the CCG.

6.2 Chief Finance Officer

In accordance with the NHS Protect Standards for Commissioners, The Chief Finance Officer has been designated as the Executive level Security Management Director to take responsibility for security management matters. The Security Management Director is answerable to the Accountable Officer as noted above.

6.3 Directors

Directors are 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 (LSMS) 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 CCG premises. They should also ensure that security implications are considered as part of tendering processes for new and existing services.

6.4 Employees

Employees have a number of duties and responsibilities regarding security. These include:

- Co-operating with management to achieve the aims of this policy, making themselves aware of any security requirements relating to their place of work or work practices and following prescribed working methods and security procedures at all times;
- Reporting all security related incidents, including violence and aggression, theft or loss through the CCGs incident reporting procedures, ensuring that line management are fully aware of the circumstances;
- Safeguard themselves, colleagues, visitors, etc., so far as is reasonably practicable;
- Be responsible for their own personal property whilst at work and to not leave such items in plain view and open to potential theft;
- Ensure the security of CCG equipment which they have responsibility or custody of;
- Ensure their ID Badge is worn and visible at all times, while on CCG premises. The Loss of an ID badge, swipe cards and access fobs must be reported immediately;
- Staff working in areas controlled by another organisation should familiarise themselves with the security procedures for that organisation.

Any deliberate or serious neglect of security measures could result in disciplinary action being taken.

6.5 Local Security Management Specialist

In accordance with the NHS Standard Contract and NHS Protect Standards, the CCG is required to nominate an individual as an accredited Local Security Management Specialist (LSMS). The specific responsibilities of the LSMS are to:

- Ensure the CCG is tackling violence against staff across the organisation, acting as lead for the reporting of all verbal and physical abuse of staff and ensuring that relevant incidents are reported to external bodies as necessary;
- The development, implementation and maintenance of an effective Security Management Policy, and other security related documents, in consultation with staff representatives, ensuring compliance with current guidance;
- To prepare a written work plan, with the Security Management Executive Director (Chief Finance Officer) and preparing regular reports on progress against that plan;
- Assist local managers in carrying out investigations into security related incidents, liaising as required with local Police, the Criminal Justice Unit and where necessary preparing case files for submission to Court as part of the prosecution process;

- Instigate regular campaigns to highlight the importance of security and the responsibilities of all CCG employees;
- Advise the CCG of any statutory requirements, and other by the preparation of procedures, for dealing with crime prevention, supply of security systems and maintenance;
- To foster links with local agencies and bodies, such as Police, Crime and Disorder Reduction Partnerships, Prevent (Counter Terrorism) leads and other security professionals in neighbouring NHS organisations;
- To develop processes and undertake monitoring of the security management arrangements of providers of NHS funded care in accordance with NHS Protect Standards for Commissioners.

Local Security Management Specialist: Gary Ross Tel: 07906 651391 Email: gary.ross@audit-one.co.uk

7. SECURITY PROCEDURES AND PROCESSES

7.1 Risks to Security

The CCG recognises that staff, patients and the public expect a safe and secure environment and should not be put at risk directly or indirectly from the effects of crime or other threats.

Crime can be a disturbing experience causing disruption and inconvenience to all concerned. For these reasons the CCG is committed to providing and maintaining a working environment that is safe and secure for all people who may be affected by its activities including employees, patients and visitors.

Criminal offences that could be considered include:

- Violence against staff by any person;
- Violence against patients by any person;
- Harassment of staff by any person;
- Kidnap of staff or their families;
- Theft of property belonging to the CCG;
- Theft of personal property belonging to staff, patients or others;
- Theft of cash, armed robbery in transit and burglary;
- Theft of information and electronic eavesdropping;
- Criminal damage to CCG property and premises (including arson);
- Criminal damage to staff property;
- Unauthorised intruders;
- Extortion, sabotage and coercion;

- Armed terrorist attack and action by criminals and activists including vehicle or pedestrian born explosive devices;

Threats to the organisation could include:

- Accidents;
- Communications failure;
- Fire including arson;
- Information destruction or corruption;
- Medical Emergencies;
- Natural disaster – flood;
- Power or critical equipment failure;
- Riot;
- Threats to personal security and safety;
- Threats to security of computer information.

7.2 Incident Reporting

All security related incidents/near misses are to be reported to local line management and the LSMS, using the CCG Datix incident reporting system form. A local investigation should then be initiated by managers.

All incidents of crime are to be reported to the Police, via either 101 or 999depending on the nature of the incident. The LSMS is also to be notified as soon as possible by telephone/e-mail.

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

- Physical assault or verbal abuse by a patient, visitor or another member of staff toward a member of staff;
- Physical assault or verbal abuse by a member of staff toward a patient or visitor;
- Theft of staff belongings or CCG property;
- Leaving workplaces open at the end of the working day;
- Damage to premises that was the result of criminal activity (including arson).

If you are in any doubt, you should contact the **Local Security Management Specialist; Gary Ross Tel: 07906 651391, Email: gary.ross@audit-one.co.uk, or the Chief Finance Officer.**

7.3 Security and Counter-Terrorism

The Office for Security and Counter Terrorism (OSCT) in the Home Office is responsible for providing strategic direction and governance on the Counter Terrorism Strategy (CONTEST 2018.) As part of CONTEST, the aim of *Prevent* is to stop people becoming radicalised/active terrorists or supporting terrorism.

CONTEST is primarily organised around four key principles. Workstreams contribute to four programmes, each with a specific objective:

- Pursue: to stop terrorist attacks;
- ***Prevent*****:** to stop people becoming terrorists or supporting terrorism;
- Protect: to strengthen our protection against a terrorist attack;
- Prepare: to mitigate the impact of a terrorist attack.

The Department of Health is a long-established partner in CONTEST through *Prevent*, Protect and Prepare. Responsibility for Pursue lies with the enforcement agencies.

Prevent objectives

Three national objectives have been identified for the *Prevent* strategy:

Objective 1: respond to the ideological challenge of terrorism and the threat we face from those who promote it;

Objective 2: prevent people from being drawn into terrorism and ensure that they are given appropriate advice and support;

Objective 3: work with sectors and institutions where there are risks of radicalisation which we need to address.

The Prevent lead for Hull CCG is the Designated Professional for Safeguarding Adults Tel: 01482 344700

The Anti-Terrorist Hotline is: 0800 789 321.

7.4 Police and Information Sharing

When a decision to contact the police has been made, the disclosure of personal information must initially be limited to that which is necessary to enable the police to identify the subject of the investigation and assess the risks. It will normally be sufficient to supply the name, date of birth, address and if required a description of the person concerned.

In the interests of public safety and the prevention of a crime, such breaches of confidentiality may be justified as being in the public interest, in accordance with the exclusion provisions of the Data Protection Act 2018 (Section 30), the Human Rights Act 1998 and the guidance given in the NHS Confidentiality Code of Practice .2003

7.5 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 their line manager/Corporate Team who will then discuss with the Local Security Management Specialist and/or Chief Finance Officer.

7.6 Personal Safety and Lone Working

Managers must ensure a risk assessment is undertaken and documented for staff considered to be lone workers or where there are potential personal safety issues. The risk assessment will include precautions to reduce the likelihood of harm occurring.

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

7.7 Premises Security

The CCG will comply with all local contractual requirements for the securing of the premises that they are based within.

7.8 Motor Vehicles

- All motor vehicles used by employees, service users, visitors and other outside agencies must park in authorised parking areas, where these have been provided.
- The security of motor vehicles owned by employees, service users and visitors is the responsibility of the owner of the vehicle.
- Providers of parking facilities will not accept liability for any theft or damage to motor vehicles or their contents when they are parked on their sites.
- CCG property is not to be left unattended in vehicles, particularly in view.
- Where it is essential that confidential documents are transported in staff cars, they must be stored in the boot of the car and remain out of sight.
- It is the responsibility of the user of a motor vehicle used on CCG business to ensure the correct public road user documents, namely a current insurance certificate or cover note, vehicle test certificate and vehicle excise licence; are valid for the vehicle, in line with the current CCG Driving Policy.

7.9 IT Security

All staff are required to comply with relevant IM&T Security Polices. It is the responsibility of all (the individual, line managers and Directors) to ensure that staff comply with these policies.

7.10 Identification Badges

ID badges are obtained via the Corporate Team. All staff must wear their ID badge at all times whilst on CCG premises, or when representing the CCG.

Managers must ensure any member of staff should hand in their ID badge (and other NHS property) on their last day of employment.

The loss of an ID Card must be reported immediately to your line manager and to the Corporate Team via Datix.

7.11 Physical Assaults, Verbal Abuse and Anti-Social Behaviour

The CCG will provide a secure environment, so far as is reasonably practicable, which protects staff and visitors from physical and verbal assaults or anti-social behaviour.

7.12 Staff Property

Secure storage for staff personal property is provided in a variety of forms which includes lockers and lockable desk drawers. The CCG will not therefore accept responsibility or liability for any unsecured articles lost or damaged in the course of duty.

Staff are advised to either take out adequate insurance against such risks if they wish their property to be covered against such losses or not bring high value items or large amounts of cash to work with them.

7.13 Lost Property

Property that has been found on the CCG premises should be reported to the Corporate Team. Any unclaimed property will be disposed of in accordance with the appropriate CCG procedure.

7.14 Access Control

It is essential that access is tightly controlled throughout the CCG premises. Where possible all access to CCG areas should be restricted. Visitors are not to be allowed to wander through premises, but should be asked to report to a reception and then met by the person who has invited them.

Outside of normal working hours, CCG premises/facilities are to be secured. Local Closedown/Lock-up procedures have been developed where this is deemed appropriate.

Some access doors have mechanical or electronic keypad entry systems to restrict access at certain times of the day or under certain circumstances. Any such doors that are part of a fire escape route will be linked to the fire alarm system to ensure they fail safe (i.e. unlock) in the event of a fire alarm.

Codes for these entry systems are only to be issued to those working in the area and must never be given to staff not working in that area. Codes must also never be given to visitors and doors with coded entry systems are never to be latched or wedged open.

Everyone should be aware of the potential for other persons ‘tailgating’ them (i.e. following without having authorisation) in order to gain access to a restricted area.

Where entry to a working area is by coded access, these codes must be changed on a regular basis, timescale to be determined by the local Corporate Team.

Departmental keys will remain under the responsibility of the relevant department and must be accounted for in an orderly system. All keys are to be held in a lockable cabinet and a record maintained of the issue and return of keys. Where such routines are not in place they are to be implemented at the earliest opportunity. Guidance on key control can be obtained from the Corporate Team.

Where members within a department/team are issued with keys to offices or areas of premises then a record of who has been issued with keys must be kept to ensure they are returned when the member of staff leaves employment with the CCG.

Some areas of CCG premises are required to be kept locked, it is therefore necessary to issue and control keys. It is vital that proper records are kept for the issuing and returning of keys. In the event of lost keys an incident/Datix report shall be completed and arrangements made to replace the key or the lock (depending on the sensitivity/nature of the area they key gave access to).

7.15 Closed Circuit Television (CCTV)

Closed circuit television cameras play an important part in crime prevention and detection in NHS premises. All cameras must comply with Home Office requirements regarding evidential value and cameras monitoring entrance/exits. All cameras should respect the right to personal privacy; operational procedures and codes of practice will govern the operation and manning of this scheme.

The objectives of CCTV are to:

- Deter and detect crime;
- Help identify, apprehend and prosecute offenders;
- Reduce theft of/from/damage to vehicles;
- Reduce the fear of crime and reassure staff, patients and visitors;
- Secure a safe environment for those working in the hospital;
- Provide assistance in Crime Prevention;
- Provide Police with evidence to take criminal / civil action in the courts;
- Assist in locating vulnerable persons.

Any CCTV systems installed in premises used by the CCG are under the control of a third party. In the event of police or other authorised body requiring CCTV data for their investigation the operator of the system should be contacted via the CCG Corporate Team.

7.16 Receipt of Goods

Any member of staff who signs for any goods on behalf of the CCG is responsible for checking the delivery for any discrepancies which may occur. All packages delivered must be identified and counted; the delivery note must not be signed unless you are sure that all items have been accounted and any discrepancies noted. Where the package is not opened but handed directly to the addressee then the addressee becomes responsible for noting any discrepancies.

Any discrepancies outstanding must be recorded accurately along with name and signature of the person delivering. Records must be updated as soon as possible, including any inventory or stock control.

7.17 Suspicious Packages and Telephone Threats

Any suspicious package must **NOT** be moved and it's position is to be immediately reported to a member of the management team. Following initial investigation (without touching or moving package) it must be established:

- Are there any wires or electronic components from the package?
- Are there any greasy/sweaty marks on the item?
- Does the package have a distinctive smell e.g. Almonds/ Marzipan?
- Enquiries are to be made in the building to identify the owner of the package.

If in doubt call the police and evacuate the immediate vicinity in line with local fire/evacuation procedure preferably without activating the fire alarm. Refer to EPRR/BCM plan if evacuation point not available due to exclusion zone.

Any suspect packages/letters are not to be placed in water, near open windows and mobile telephones should not be used near it.

Any member of staff receiving a telephone threat regarding a suspect package or an explosive device should try obtaining as much detail regarding the threat as possible. The Police must be informed immediately, along with a line/local manager. A decision will be taken by directors as whether an emergency should be declared and whether the CCGs EPRR/BCM plan is activated.

7.18 Information Security

All staff must abide by the Confidentiality Code of Conduct 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 2018 (DPA 2018)

- General Date Protection Regulations 2016 (GDPR 2016)
- The Computer Misuse Act 1990;
- Copyrights and Patents Act 1998;
- The Human Rights Act 1998.

There are Information Governance policies available which can be referred to on the Hull CCG website. Please familiarise yourself with these.

7.19 Anti-Fraud, Bribery & Corruption

It is the responsibility of all employees to be alert to the possibility of fraud being perpetrated against the CCG. Fraud costs the NHS an estimated £2billion+ per year. Fraud can best be defined as obtaining a financial benefit by deception and dishonesty. Typical examples of fraud against the CCG are as follows:

7.19.1 Contractors

- Claiming for goods/services not provided.

Service Users

- Claiming exemptions that not entitled to (e.g. free prescription).
- Claiming for expenses not entitled to.

7.19.2 Staff

- Working elsewhere while sick.
- Claiming for work not done (Timesheet fraud).
- Claiming for Travel/other expenses not incurred.

This list is not exhaustive but if any member of staff has any suspicion that fraud may be occurring against the CCG they should refer to the Fraud, Bribery and Corruption Policy and contact one of the following:-

- Chief Finance Officer
- Local Counter Fraud Specialist (Via AuditOne)

While all information will be kept strictly confidential if staff wish to report their suspicion anonymously they can contact the following:

NHS Fraud and Corruption Hotline on 0800 028 4060

8. IMPLEMENTATION

The Chief Finance Officer will ensure that a copy of this policy is freely available to all CCG staff – an electronic copy is available via the CCG website at: http://www.hullccg.nhs.uk/corporate-policies

9. TRAINING AND AWARENESS

9.1 Health and Safety awareness is a statutory requirement and therefore mandatory for all staff of the CCG (aspects of security training cut across health and safety training). The Health and Safety Policy is available on the CCG website.

9.2 All new permanent employees must comply with the Induction Policy at the earliest practicable time after commencing employment. Where necessary and/or appropriate staff will be given a local induction where they will be informed of specific health and safety related hazards and controls.

9.3 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 actually attend. Once training needs have been recognised, the manager will then make arrangements for the member of staff to undertake the next available course.

9.4 Managers are also responsible for keeping records of security training for all their members of staff.

9.5 Staff should also undertake any available e-learning modules relating to security management.

9.6 Manager are to receive the appropriate advice to ensure the content of this Policy is fully implemented.

9.7 Members of staff, identified via a valid role risk assessment, should be provided with appropriate levels of Conflict Resolution Training applicable to their role/function, in order to allow them to minimise/mitigate the risks associated with abuse, aggression and violence.

10. MONITORING AND EFFECTIVESNESS

The effectiveness of this Policy will be monitored by Health, Safety and Security Meeting.

11. POLICY REVIEW

This Policy will be reviewed within two (2) years from the date of implementation.

12. REFERENCES

- Health and Safety at Work etc. Act 1974
- Workplace Health, Safety and Welfare Regulations 1992
- Management of Health and Safety at Work Regulations 1999
- Protection from Harassment Act 1997
- Human Rights Act 1998 (in particular Article 8 “Human Rights Bill 1998 - the right to respect for private and family life”)

- Crime and Disorder Act 1998
- Freedom of Information Act 2000
- General Data protection Regulations 2016
- Data Protection Act 2018
- NHS Standard Contract 2018-19
- NHS Protect Standards for Commissioners (updated and published annually)

13. ASSOCIATED DOCUMENTATION

- Lone Workers Policy
- Risk Management Strategy
- Grievance Policy
- Whistle Blowing Policy
- Confidentiality Code of Conduct Policy
- Bullying and Harassment Policy
- Health and Safety Policy
- Information Governance Policy
- Information Security Policy
- Fire Safety Policy
- Anti-Fraud, Bribery and Corruption Policy
- Equality and Diversity Policy
- EPRR/BCM

14. APPENDICES

APPENDIX A – EQUALITY IMPACT ASSESSMENT

HR/Corporate Policy Equality Impact Analysis:	
Policy:	Security Management Policy
Date of Analysis:	June to October 2018
Completed by:	Gary Ross, Local Security Management Specialist, AuditOne.
What are the aims and intended effects of this policy, project or function?	To provide all staff, regardless of their role, function, or position, with a clear understanding of their responsibilities in ensuring a safe and secure working environment.
Are there any significant changes to previous policy likely to have an impact on staff / other stakeholder groups?	The significant changes affecting this policy compared to its predecessor document relates to the demise of the NHS Protect and its role as a regulatory body with oversight responsibilities for the NHS Protect Standards for Commissioners on Security Management Standards & the appropriate provisions of the NHS Standard Contract.
Please list any other policies that are related to or referred to as part of this analysis	▪ Lone Workers Policy ▪ Risk Management Strategy ▪ Grievance Policy ▪ Whistle Blowing Policy ▪ Confidentiality Code of Conduct Policy ▪ Bullying and Harassment Policy ▪ Health and Safety Policy ▪ Information Governance Policy ▪ Information Security Policy ▪ Fire Safety Policy

	▪ Anti-Fraud, Bribery and Corruptio Policy
Who will the policy, project or function affect?	Any/all Hull CCG members of permanent, part-time & bank members of staff and contractors.
What engagement/consultation has been done, or is planned for this policy and the equality impact assessment?	
Promoting Inclusivity and Hull CCG's Equality Objectives. How does the project, service or function contribute towards our aims of eliminating discrimination and promoting equality and diversity within our organisation? How does the policy promote our equality objectives: 1. Ensure patients and public have improved access to information and minimise communications barriers 2. To ensure and provide evidence that equality is consciously considered in all commissioning activities and ownership of this is part of everyone's day-to-day job 3. Recruit and maintain a well-supported, skilled workforce, which is representative of the population we serve 4. Ensure the that NHS Hull Clinical Commissioning Group is welcoming and inclusive to people from all backgrounds and with a range of access needs	By providing all members of staff with knowledge, understanding and a framework for ensuring their safety and security whilst at work.

Equality Data	
Is any Equality Data available relating to the use or implementation of this policy, project or function? Equality data is internal or external	Yes □ No ☒

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: Recruitment data, e.g. applications compared to the population profile, application success rates 2: Complaints by groups who share / represent protected characteristics 4: Grievances or decisions upheld and dismissed by protected characteristic group 5: Insight gained through engagement	Where you have answered yes, please incorporate this data when performing the *Equality Impact Assessment Test* (the next section of this document). If you answered No, what information will you use to assess impact? **Please note that due to the small number of staff employed by the CCG, data with returns small enough to identity individuals cannot be published. However, the data should still be analysed as part of the EIA process, and where it is possible to identify trends or issues, these should be recorded in the EIA.**

Assessing Impact

Is this policy (or the implementation of this policy) likely to have a particular impact on any of the protected characteristic groups?
(Based on analysis of the data / insights gathered through engagement, or your knowledge of the substance of this policy)

Protected Characteristic:	No Impact:	Positive Impact:	Negative Impact:	Evidence of impact and, if applicable, justification where a ***Genuine Determining Reason***[1] exists (see footnote below – seek further advice in this case)
Gender	X			The application of this policy is both fair and consistent regardless of the gender and therefore does not impact on this protected characteristic
Age	X			The application of this policy is both fair and consistent regardless of the age and therefore does not impact on this protected characteristic
Race / ethnicity / nationality	X			The application of this policy is both fair and consistent regardless of the race, ethnicity or nationality of the person and therefore does not

1. [1] *The action is proportionate to the legitimate aims of the organisation (please seek further advice)*

				impact on this protected characteristic
Disability	X			The application of this policy is both fair and consistent regardless of the physical status of the individual and therefore does not impact on this protected characteristic
Religion or Belief	X			The application of this policy is both fair and consistent regardless of the belief system of the person and therefore does not impact on this protected characteristic
Sexual Orientation	X			The application of this policy is both fair and consistent regardless of the sexual orientation of the individual and therefore does not impact on this protected characteristic
Pregnancy and Maternity	X			The application of this policy is both fair and consistent regardless of the status of the person and therefore does not impact on this protected characteristic
Transgender/Gender reassignment	X			The application of this policy is both fair and consistent regardless of the gender of the individual and therefore does not impact on this protected characteristic
Marriage or civil partnership	X			The application of this policy is both fair and consistent regardless of the marital status of the individual and therefore does not impact on this protected characteristic

Action Planning:

As a result of performing this analysis, what actions are proposed to remove or reduce any risks of adverse impact or strengthen the promotion of equality?

Identified Risk:	**Recommended Actions:**	**Responsible Lead:**	**Completion Date:**	**Review Date:**

APPENDIX B – KEY GUIDANCE

NHS Standard Contract and NHS Protect Standards for Commissioners on Security Management

Guidance on NHS Standard Contract stipulations (including Service Condition 24 which details provider security management and counter fraud arrangements) can be viewed at https://www.england.nhs.uk/nhs-standard-contract/

The applicable standards for security management (and also for fraud, bribery and corruption) can be viewed at http://www.nhsbsa.nhs.uk/3577.aspx. Each standards document is set out in four sections and covers corporate responsibilities and key principles for action. These are:

- Strategic governance sets out the requirements in relation to the strategic governance arrangements of the organisation to ensure that anti-crime measures are embedded at all levels across the organisation.
- Inform and Involve sets out the requirements in relation to raising awareness of crime risks against the NHS and working with NHS staff and the public to publicise the risks and effects of crime against the NHS.
- Prevent and Deter sets out the requirements in relation to discouraging individuals who may be tempted to commit crime against the NHS and ensuring that opportunities for crime to occur are minimised.
- Hold to Account sets out the requirements in relation to detecting and investigating crime, prosecuting those who have committed crimes, and seeking redress.

There will be a quality assurance process for commissioners in respect of their anti-crime arrangements including Security Management. This is detailed within the NHS Protect Standards for Commissioners (link noted above) and updated at each annual publication.

APPENDIX C – SIGN OFF

Sign-off
All policy EIAs must be signed off by Mike Napier, Associate Director of Corporate Affairs
I agree with this assessment / action plan
If *disagree*, state action/s required, reasons and details of who is to carry them out with timescales:
Signed:
Date:03.01.19