

## SECURITY MANAGEMENT POLICY

**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:	July 2016
Date to be reviewed:	July 2017; thereafter every 2 years

<b>Policy Title:</b>	Security Management Policy	
<b>Supersedes:</b>	NHS Hull Security Policy (PCT Policy - 2011)	
<b>Description of Amendment(s):</b>	New policy based on NHS Protect Standards for Commissioners first issued in 2015	
<b>This policy will impact on:</b>	All CCG employees on permanent or temporary contracts (including Board members) and bank or agency staff	
<b>Financial Implications:</b>	None	
<b>Policy Area:</b>	Finance	
<b>Version No:</b>	1.0	
<b>Issued By:</b>	Integrated Audit and Governance Committee Responsible Director: Emma Sayner – Chief Finance Officer	
<b>Author:</b>	Shaun Fleming Local Security Management Specialist	
<b>Document Reference:</b>		
<b>Effective Date:</b>	July 2016	
<b>Review Date:</b>	July 2017 then every two years thereafter	
<b>Impact Assessment Date:</b>		
<b>APPROVAL RECORD</b>	Health and Safety Group	21 <sup>st</sup> June 2016
	Integrated Audit and Governance Committee	12 <sup>th</sup> July 2016
<b>Consultation:</b>	Staff consultation via email	27 <sup>th</sup> June 2016

# CONTENTS

INTRODUCTION .....	3
PURPOSE.....	3
SCOPE .....	3
DUTIES OF THE ORGANISATION .....	4
OVERVIEW.....	4
THE ACCOUNTABLE OFFICER.....	4
SECURITY MANAGEMENT DIRECTOR .....	4
DIRECTORS .....	4
LOCAL SECURITY MANAGEMENT SPECIALIST (LSMS) .....	5
MANAGERS.....	5
CCG STAFF .....	6
KEY PERFORMANCE INDICATORS .....	6
SECURITY PROCEDURES AND PROCESSES.....	7
POLICY DEVELOPMENT .....	14
DISSEMINATION AND IMPLEMENTATION PROCESS, INCLUDING TRAINING .....	15
LIBRARY AND ARCHIVING ARRANGEMENTS .....	15
APPENDIX A: NHS STANDARD CONTRACT AND NHS PROTECT STANDARDS FOR COMMISSIONERS 2016/17	
EQUALITY IMPACT ASSESSMENT TOOL	

## Introduction

This document is issued in accordance with guidance from NHS Protect and the NHS Protect Standards for Commissioners, published annually and issued to NHS Bodies, on measures to deal with theft, violence against NHS Staff, and 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.

It defines the main functions and responsibilities of those involved in implementing the policy. This document is to be brought to the attention of every employee and should be read carefully with its principles adhered to.

## Purpose

The purpose of this policy is to detail NHS Hull CCG's responsibility for the effective management of security in relation to staff, patients, 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 and ensure a robust response in line with the national NHS Protect policies;
- 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 premises, staff, patients and visitors.

## Scope

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

## Duties of the Organisation

### OVERVIEW

NHS Hull CCG recognises that the corporate responsibility for security management lies with Senior Executives who are charged with managing business affairs. The NHS Protect Standards for Commissioners requires that there is an Executive Director nominated as the Security Management Director and that a Local Security Management Specialist is nominated, trained and accredited by NHS Protect. Counter terrorism (Security Act 2015) is delivered through the Prevent initiative and details of the CCG Prevent lead key contact is noted in this document below under 'Security and Counter Terrorism'.

### THE 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.

### SECURITY MANAGEMENT DIRECTOR

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.

NHS Protect will be informed of these designations and of any ongoing changes.

### 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.

## LOCAL SECURITY MANAGEMENT SPECIALIST (LSMS)

In accordance with the NHS Standard Contract and NHS Protect Standards, the CCG is required to nominate an individual as the Local Security Management Specialist. NHS Protect are to be informed of any such nomination. The nominated individual must be accredited by NHS Protect to undertake the LSMS role. The specific responsibilities of the LSMS are:

- 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 the Legal Protection 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: Shaun Fleming Tel: 01482 866800 Email: [shaunfleming@nhs.net](mailto:shaunfleming@nhs.net)**

## MANAGERS

Managers on behalf of their Directors are responsible for:

- Ensuring compliance with the CCG Security Policy requirements in the areas for which they are responsible;
- Ensuring so far as is reasonable practicable the areas under their control are safe and secure;
- Ensure risks and procedures are explained in local on-site induction;
- Develop, where necessary local security procedures for their departments and other areas of responsibility, based on the overall CCG Security Policy;

- Ensuring risk assessments are undertaken on all potential security hazards;
- Lone workers;
- Any members of staff dealing with patients and carers, security of IT equipment, buildings and premises, loss of ID badges;
- Ensuring all security incidents are appropriately reported and investigated;
- Ensure compliance with local procedures and documented arrangements to retrieve equipment and ID badges, keys and access fobs etc. from staff leaving the organisation.

## CCG STAFF

Members of staff 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.

## KEY PERFORMANCE INDICATORS

The introduction of self-assessment SRT (Self Review Tool) Quality Standards, by NHS Protect, in support of NHS Protect Standards for Commissioners will inform and help determine CCG Security KPI's – see Appendix A. The first SRT submission is expected to be completed by the organisation (LSMS as Lead) by November 2016.

## Security Procedures and Processes

### 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.

## Incident Reporting

---

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

All incidents of crime are to be reported to the local Police Station. 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 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: Shaun Fleming Tel: 01482 866800 Email: [shaunfleming@nhs.net](mailto:shaunfleming@nhs.net)** or the Chief Finance Officer.

## 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.) As part of CONTEST, the aim of *Prevent* is to stop people becoming 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 Dave Blain Designated Professional for Safeguarding Adults 07802 718233 [d.blain@nhs.net](mailto:d.blain@nhs.net)**

**The Anti-Terrorist Hotline is: 0800 789 321.**

---

## 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 1998 (Section 29), the Human Rights Act 1998 and the guidance given in the NHS Confidentiality Code of Practice.

## 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.

---

## Personal Safety & 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.

---

## Premises Security

---

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

## Motor Vehicles (including Security)

---

- 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.

## IT Security

---

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

## 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 badge must be reported immediately to your manager and the Corporate Team. An incident form must be completed.

## Physical and Verbal Assaults/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. The CCG has a Management of Violence and Aggression Policy.

## 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.

---

## Lost Property

---

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

---

## 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 patients or 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' (i.e. following without having authorisation) them 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 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).

### 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.

### 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.

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.

### Suspicious Packages and Telephone Threats

---

Any suspicious package must **NOT** be moved and its position is to be reported to management. 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.

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 emergency plan is activated.

## 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 1998;
- 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 internet. Please familiarise yourself with these.

## Anti-Fraud, Bribery and 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:

### 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.

### 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 (Nikki Cooper/Shawn Fleming Tel:01482 866800)

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

**NHS Fraud and Corruption Hotline on  
0800 028 4060**

## Training

---

The content of this policy will form part of the CCG Induction Programme. In addition to this:

- Managers are to receive the appropriate advice to ensure the content of this policy is fully implemented;
- Employers should provide frontline staff with Conflict Resolution Training where considered relevant or appropriate. This training will provide all staff with the theory behind violence at work, so that they understand why it occurs and how any individual can be a potential aggressor given a set of circumstances.
- It is also extremely important that staff know how their actions may contribute to or exacerbate a threatening or violent situation/incident.

## Policy Development

Consultation and communication with stakeholders during development.

## Approval and ratification process

---

All non-clinical policies must be formally ratified by the appropriate Committee before implementation. This policy will be formally approved by the NHS Hull CCG board.

## Owner and version control/review process

---

The CCG Local Security Management Specialist is the owner of this policy. This policy will be reviewed after one year. If there are no major changes after the first year, then following review a date will be set at 2 years, with the agreement of the owning Group or Committee. However, it is the Policy Owners responsibility to review their policy if there are changes before the review date is met.

## Dissemination and Implementation Process, including training

### Dissemination and 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>

### Training

---

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.

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.

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.

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

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

## Library and archiving arrangements

The Chief Finance Officer will ensure the latest version of the policy is available to all staff in compliance with national/NHS policy retention guidelines.

This policy will supersede any older NHS Hull CCG Security Management Policies, and these will be archived in accordance with local guidance and procedures. Existing security risk assessments can remain in use until they are reviewed, then the information will be transferred into the new documentation, and the old assessment archived.

### Monitoring of Compliance and effectiveness

---

The Chief Finance Officer will ensure the processes outlined in this policy and any associated policies and guidance are followed.

## Associated Documents and Policies

---

- 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

## References

---

### References

- Health and Safety at Work etc. Act 1974
- Management of Health and Safety at Work Regulations 1999
- NHS Standard 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 (updated and published annually)

## Appendix A – 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.

## Equality Impact Analysis:

<b>Policy / Project / Function:</b>	Security Management Policy								
<b>Date of Analysis:</b>	July 2016								
<b>This Equality Impact Analysis was completed by: (Name and Department)</b>	Shaun Fleming Local Security Management Specialist								
<b>What are the aims and intended effects of this policy, project or function?</b>	Produce a Security Management Policy in compliance with NHS Protect Standards on Security Management for commissioners.								
<b>Please list any other policies that are related to or referred to as part of this analysis</b>	<ul style="list-style-type: none"> <li>▪ Lone Workers Policy</li> <li>▪ Risk Management Strategy</li> <li>▪ Grievance Policy</li> <li>▪ Whistle Blowing Policy</li> <li>▪ Confidentiality Code of Conduct Policy</li> <li>▪ Bullying and Harassment Policy</li> <li>▪ Health and Safety Policy</li> <li>▪ Information Governance Policy</li> <li>▪ Information Security Policy</li> <li>▪ Fire Safety Policy</li> <li>▪ Anti-Fraud, Bribery and Corruption Policy</li> </ul>								
<b>Who does the policy, project or function affect ?</b>  Please Tick ✓	<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 60%;">Employees</td> <td style="width: 40%; text-align: center;"><input checked="" type="checkbox"/></td> </tr> <tr> <td>Service Users</td> <td style="text-align: center;"><input type="checkbox"/></td> </tr> <tr> <td>Members of the Public</td> <td style="text-align: center;"><input type="checkbox"/></td> </tr> <tr> <td>Other (List Below)</td> <td style="text-align: center;"><input type="checkbox"/></td> </tr> </table>	Employees	<input checked="" type="checkbox"/>	Service Users	<input type="checkbox"/>	Members of the Public	<input type="checkbox"/>	Other (List Below)	<input type="checkbox"/>
Employees	<input checked="" type="checkbox"/>								
Service Users	<input type="checkbox"/>								
Members of the Public	<input type="checkbox"/>								
Other (List Below)	<input type="checkbox"/>								

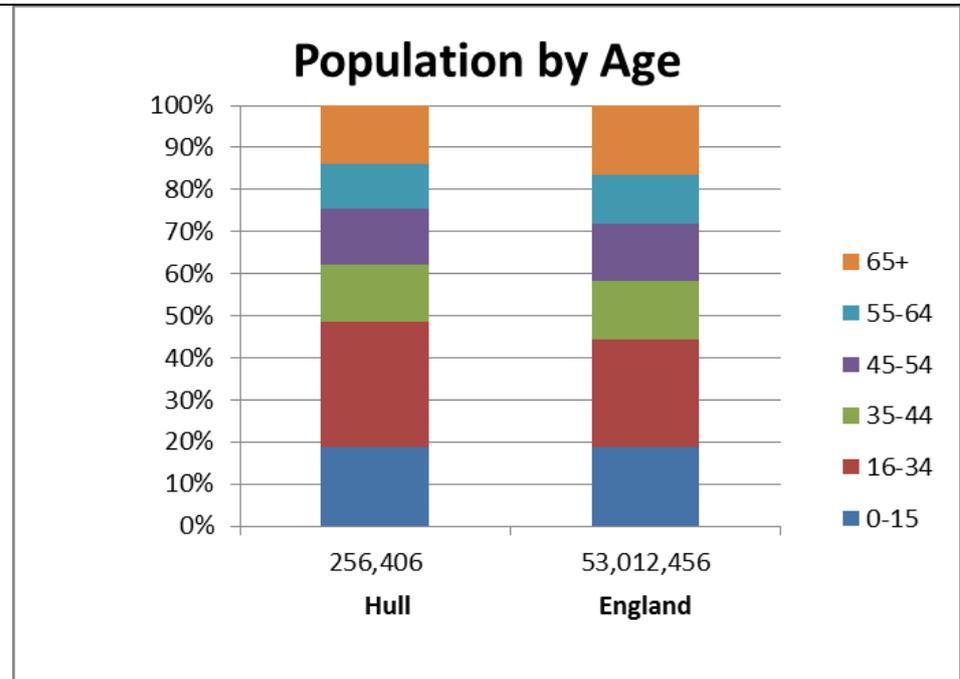
## Equality Impact Analysis:

**Local Profile/Demography of the Groups affected** (population figures) Relevant data can be found in the attached Knowledge Management Toolkit

### General

There are 51 GP practices in the Hull area which spans 7,154 hectares and, as a city, has relatively tight geographical boundaries with most of the 'leafy suburb' areas outside Hull's boundaries in East Riding of Yorkshire. As a result, Hull has a relatively high deprivation score, as measured by the Index of Multiple Deprivation 2010, with Hull ranked as the 10th most deprived local authority out of 326 (bottom 4%). The resident population of Hull is 256,406 based on the 2011 Census data and 265,369 residents based on estimates from the local GP registration file as at October 2011. This equates to approximately 37 residents per hectare. The Joint Strategic Needs Assessment (JSNA) identifies considerable inequalities in health between Hull and England, and between populations within Hull.

### Age



Compared to England, Hull has lower percentages of residents aged 10-19 years and 55+ years, but slightly higher percentages aged under 5, 20-34 years and 45-54 years. There is a relatively large difference between Hull and England for the age group 20-34 years, due to Hull's colleges and Universities.

There were 2,869 live births occurring to Hull residents in 2001, but this has increased steadily to 3,771 for 2010. The number of deaths occurring to Hull residents has decreased from 2,571 to 2,310 between 2001 and 2010. ONS estimated the resident population to be 243,596 in 2001 compared to 260,424 residents based on the GP registration file, with the difference between these estimates narrowing over time. So, whilst it is difficult to quantify the exact increase in Hull's population, it has increased over recent years. Between 2010 and 2030, ONS

	<p>estimate that Hull's population will increase from 266,100 to 311,900 residents, an increase of 17%.</p> <p>The figure above shows the population of Hull (2011 Census Data).</p>																				
<b>Race</b>	<p>The percentage of the population from Black and Minority Ethnic (BME) groups has increased substantially since 2001. For the 2001 Census, it was estimated that 3.3% of Hull's population was not White British or White Irish, whereas Census data shows that this figure increased to 10.2% for 2011. There is no single BME group in Hull with much higher percentages compared to other groups. The 2011 census data shows:</p> <p>White British - 89.7%  White Other - 4.4%  Mixed – 1.3%  Asian - 2.5%  Black - 1.2%  Other – 0.8%</p>																				
<b>Sex</b>	<p>The gender split in Hull is approximately 50.1% men and 49.9% women. For 2008-2010, life expectancy in Hull was 75.7 years for men and 80.2 years for women compared to 78.6 years and 82.6 years for men and women respectively in England.</p>																				
<b>Gender reassignment</b>	<p>No local information provided.</p>																				
<b>Disability</b>	<p>According to the 2011 Census, it is estimated that approximately 19.7% of the Hull population lives with a long term health problem or disability compared with 17.6% for England. This information can be broken down further (Source: Projecting Older People Population Information System and Projecting Adult Needs and Service Information) to include learning disabilities, physical disabilities, hearing impairments and visual impairments, as follows:</p> <p>2012 Estimates – Hull</p> <table> <tr> <td>Learning Disability (Age 18-64)</td> <td>4,078</td> </tr> <tr> <td>Learning Disability 65+</td> <td>762</td> </tr> <tr> <td>Physical Disability (Moderate 18-64)</td> <td>12,222</td> </tr> <tr> <td>Physical Disability (Serious 18-64)</td> <td>3,491</td> </tr> <tr> <td>Visual Impairment (Age 18-64)</td> <td>108</td> </tr> <tr> <td>Visual Impairment 65+</td> <td>3,263</td> </tr> <tr> <td>Hearing Impairment (Moderate/Severe 18-64)</td> <td>5,765</td> </tr> <tr> <td>Hearing Impairment (Moderate/Severe 65+)</td> <td>15,707</td> </tr> <tr> <td>Hearing Impairment (Profound 18-64)</td> <td>49</td> </tr> <tr> <td>Hearing Impairment (Profound 65+)</td> <td>402</td> </tr> </table>	Learning Disability (Age 18-64)	4,078	Learning Disability 65+	762	Physical Disability (Moderate 18-64)	12,222	Physical Disability (Serious 18-64)	3,491	Visual Impairment (Age 18-64)	108	Visual Impairment 65+	3,263	Hearing Impairment (Moderate/Severe 18-64)	5,765	Hearing Impairment (Moderate/Severe 65+)	15,707	Hearing Impairment (Profound 18-64)	49	Hearing Impairment (Profound 65+)	402
Learning Disability (Age 18-64)	4,078																				
Learning Disability 65+	762																				
Physical Disability (Moderate 18-64)	12,222																				
Physical Disability (Serious 18-64)	3,491																				
Visual Impairment (Age 18-64)	108																				
Visual Impairment 65+	3,263																				
Hearing Impairment (Moderate/Severe 18-64)	5,765																				
Hearing Impairment (Moderate/Severe 65+)	15,707																				
Hearing Impairment (Profound 18-64)	49																				
Hearing Impairment (Profound 65+)	402																				
<b>Sexual Orientation</b>	<p>There are no local statistics for how many Lesbian, Gay or Bisexual (LGB) people live within Hull however, nationally, the Government estimates that 5% of the population are lesbian, gay, bi and transgender communities.</p>																				
<b>Religion, faith and belief</b>	<p>According to the 2011 Census, 54.9% of the population have identified themselves as Christian and 3.1% of the population is made up of other religions. The remainder of the population did not state anything (7.2%) or stated 'no religion' (34.8%).</p>																				

<b>Marriage and civil partnership</b>	This protected characteristic generally only applies in the workplace. Data from the Office of National Statistics covering the period 2008-2010 indicates that there were 18,049 Civil Partnerships in England and Wales during this three-year period – 52% men and 48% women.
<b>Pregnancy and maternity</b>	There were 2,869 live births occurring to Hull residents in 2001, but this has increased steadily to 3,771 for 2010.

Equality Impact Analysis:	
<p><b>Is any Equality Data available relating to the use or implementation of this policy, project or function ?</b></p> <p>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 <i>Protected Characteristics</i> – referred to hereafter as ‘<i>Equality Groups</i>’.</p> <p>Examples of <i>Equality Data</i> include: (this list is not definitive)</p> <p>1: Application success rates <i>Equality Groups</i>  2: Complaints by <i>Equality Groups</i>  3: Service usage and withdrawal of services by <i>Equality Groups</i>  4: Grievances or decisions upheld and dismissed by <i>Equality Groups</i></p>	<p>Yes <input type="checkbox"/></p> <p>No <input checked="" type="checkbox"/></p> <p>Where you have answered yes, please incorporate this data when performing the <i>Equality Impact Assessment Test</i> (the next section of this document).</p>
<p><b>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</b></p>	<p>Consultation has taken place locally with staff and within the organisation:</p> <ul style="list-style-type: none"> <li><input type="checkbox"/> CCG Employees</li> <li><input type="checkbox"/> Health, Safety and Security Group</li> <li><input type="checkbox"/> Integrated Audit and Governance Committee</li> </ul>

<p><b>Promoting Inclusivity</b></p> <p>How does the project, service or function contribute towards our aims of eliminating discrimination and promoting equality and diversity within our organisation</p>	<p>The policy contributes to promoting equality and diversity by providing a framework for equitable application of security management processes and procedures.</p>
---	---

## Equality Impact 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 <i>Genuine Determining Reason</i> exists
<b>Gender</b> (Men and Women)	✓			Application of the policy is fair and consistent regardless of gender and therefore does not impact on this protected characteristic.
<b>Race</b> (All Racial Groups)	✓			Application of the policy is fair and consistent and therefore does not impact on this protected characteristic.
<b>Disability</b> (Mental and Physical)	✓			Application of the policy is fair and consistent and therefore does not impact on this protected characteristic.
<b>Religion or Belief</b>	✓			Application of the policy is fair and consistent regardless of religion or belief and therefore does not impact on this protected characteristic.
<b>Sexual Orientation</b> (Heterosexual, Homosexual and Bisexual)	✓			Application of the policy is fair and consistent regardless of sexual orientation and therefore does not impact on this protected characteristic.
<b>Pregnancy and Maternity</b>	✓			Application of the policy is fair and consistent and therefore does not impact on this protected characteristic.

<b>Transgender</b>	✓			Application of the policy is fair and consistent and therefore does not impact on this protected characteristic.
<b>Marital Status</b>	✓			Application of the policy is fair and consistent regardless of marital status and therefore does not impact on this protected characteristic.
<b>Age</b>	✓			Application of the policy is fair and consistent 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 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:

## Equality Impact Findings:

<b>Analysis Rating:</b>	Green
<b>Red – Stop and remove the policy</b>	<b>Red:</b> 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 <i>Protected Characteristics</i> . It is recommended that the use of the policy be suspended until further work or analysis is performed.
<b>Red Amber – Continue the policy</b>	<b>Red Amber:</b> 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 <i>Protected Characteristics</i> . However, a genuine determining reason may exist that could legitimise or justify the use of this policy and further professional advice should be taken.
<b>Amber – Adjust the Policy</b>	<b>Amber:</b> 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 <i>Action Planning</i> section of this document.
<b>Green – No major change</b>	<b>Green:</b> As a result of performing the analysis, the policy, project or function does not appear to have any adverse effects on people who share <i>Protected Characteristics</i> and no further actions are recommended at this stage.

<b>Other Comments:</b>	
<b>Confirmed by (Manager): (Name and Title)</b>	

	
<b>Date:</b>	09.08.16