Castle Point and Rochford
Clinical Commissioning Group

SECURITY POLICY

Policy Number:	CPRCCG CP15
Version:	3.0
Ratified By:	NHS Castle Point & Rochford CCG Governing Body
Date Ratified:	28th November 2019
Name of Sponsor:	Director of Strategy & Planning
Name of Originator/Author:	Local Security Management Specialist
Date Issued:	November 2019
Review Date:	November 2021
Target Audience:	CCG Staff and Members

1.0 INTRODUCTION AND POLICY STATEMENT

1.1 It is the policy of Castle Point and Rochford CCG to provide a safe environment for staff, volunteers, patients, visitors and others legally on the CCG premises, as far as reasonably practicable. It is recognised that the CCG Security Policy must not impede the public right of access or have a negative effect on privacy or quality of care. Security arrangements shall integrate with Health & Safety and Fraud, Bribery & Corruption procedures.

1.2 This document is issued in accordance with guidance within the NHS Standard Contract (Standard Commissioning Contract), available to NHS Bodies, on measures to deal with violence against NHS Staff, and security matters. The policy covers the general security arrangements within the organisation and notes the relationship with other security related policies.

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

2.0 PURPOSE

2.1 The purpose of this policy is to detail Castle Point and Rochford 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 encourage:-

- Strategic Governance - This area ensure that security management is embedded throughout the organisation, with focus on the SMD and LSMS. The aim is to ensure that anti-crime measures are embedded at all levels across the organisation.
- Inform and Involve – This area sets out the requirements in relation to raising awareness of crime risks against the NHS and working with NHS staff, stakeholders and the public to highlight the risks and consequences of crime against the NHS.
- Prevent and Deter - This area sets out the requirements in relation to discouraging individuals who may be tempted to commit crimes against the NHS and ensuring that opportunities for crime to occur are minimised.
- Hold to Account - This section sets out the requirements in relation to detecting and investigating crime, prosecuting those who have committed crimes and seeking redress.

Through developing a culture which recognises the importance of security Castle Point and Rochford CCG will be able to:

- 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 CCG's Disciplinary Policy.

- 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

This policy is concerned with:

- The protection of persons and property
- The prevention and detection of crime

3.0 DUTIES OF THE ORGANISATION

3.1 Overview

NHS Castle Point and Rochford CCG recognises that the corporate responsibility for security management lies with Senior Executives who are charged with managing business affairs. The NHS Standard Contract requires that there is an Executive Director nominated as the Security Management Director, a non-Executive Director is nominated to provide independent oversight of security and a Local Security Management Specialist is nominated, trained and accredited.

3.2 The Accountable Officer

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

3.3 Security Management Director (SMD)

In accordance with the Directors, The Director of Strategy and Planning has been designated as the Executive Director to take responsibility for security management matters. A Non-Executive Director has also been designated to promote security management measures.

3.4 Directors

Directors on behalf of the Chief Executive are responsible for ensuring that the CCG's Security Policy is implemented within the organisation.

This will include the responsibility for:

- Ensuring they are confident and aware of the CCG's security risks, controls in place to mitigate these risks and what action plans are in place to reduce crime risks.
- 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 with the CCG's premises. They should also ensure that security implications are considered as part of tendering processes for new and existing services.

3.5 Local Security Management Specialist (LSMS)

In accordance with the Directions, the CCG is required to nominate an individual as the Local Security Management Specialist. The nominated individual must be accredited to undertake the LSMS role and prepare an annual work programme to help meet defined national security standards. The specific responsibilities of the LSMS are:

- Ensure that security management work, including incident reporting and risk assessment, is integrated into systems for risk management throughout the organisation.
- Support managers and their staff with casework for potential criminal proceeding.
- 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.
- Development, implement and maintain an effective Security 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 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 and other security professionals in neighbouring NHS organisations

3.6 Managers

Managers are required to exercise preventative aspects and to take appropriate action where necessary in respect of those who offend against the law, commit misconduct or other breach of security in contravention of the policies of the service.

Managers on behalf of their Directors are responsible for:

- Making sure they are fully aware of and understand the policies and procedures for security, the contingency plans and know their role within the plan.

- Ensuring all staff are aware of their roles and exercise good security practice.
- Ensuring that any local CCTV system and videotape handling and storage is done in accordance with the requirements of Data Protection and Human Rights Acts.
- Ensuring compliance with the CCG Security Policy requirements in the areas for which they are responsible.
- Ensuring so far as is reasonable practicable that the areas under their control are safe and secure.
- Ensure risks and procedures are explained in local on-site induction and identify training requirements for staff there after.
- Develop, where necessary local security procedures for their departments and other areas of responsibility, based on the overall CCG Security Policy.
- Ensuring that risk assessments are undertaken on all potential security hazards, including, but not limited to 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 to LSMS and investigated.
- Ensure that sound arrangements are in place to retrieve equipment and ID badges, keys and access fobs etc. from staff leaving the organisation.

3.7 CCG Staff

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

- Complying with security procedures relevant to their workplace.
- Familiarising themselves with local security risks and controls. This can be achieved through attending relevant training to increase knowledge.
- 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 CCG' s incident reporting procedures, ensuring that line management are fully aware of the circumstances. Advice on how to report can be found in this policy under Incident Reporting page 9.
- 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 that that 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.
- Comply with all training requirements concerning security issues.

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

3.6 Staff from other organisations

Staff from other CCG's and/or other organisations should be aware of the details of the CCG's Security related policies and procedures as well as those of their own employers. Where required Castle Point and Rochford CCG will ensure adequate liaison is established between other bodies to ensure consistency of procedures and guidelines.

CCG staff working at or visiting the premises of other organisations should familiarise themselves with the security arrangements for the location they are visiting.

3.7 Key Performance Indicators

This policy will be regularly monitored to ensure that it is effective. The following performance indicators will be used as part of that evaluation:

- Baseline information from the incident reporting procedures.
- A demonstrable reduction (over time) in the number of security incidents reported.
- A positive evaluation of the effectiveness of training programmes.
- Development of security work plan and implementation of identified activities.

4.0 SECURITY PROCEDURES AND PROCESSES

4.1 Risk 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
- Harassment of staff by any person
- Theft of property belonging to the CCG
- Theft of personal property belonging to staff, patients or others
- Theft of information and electronic eavesdropping
- Criminal damage to CCG property and premises (including arson)
- Criminal damage to staff property
- Unauthorised intruders

Threats to NHS organisations could include:

- Accidents
- Communications failure
- Fire including arson
- Information destruction or corruption
- Medical Emergencies

- Natural disaster - flood
- Suicide
- Power or critical equipment failure
- Riot
- Threats to personal security and safety
- Threats to security of computer information

4.2 Incident Reporting

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

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

The LSMS must be informed of any assault to a member of staff, as soon as possible following the event.

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 LSMS.

Your LSMS contacts is:
John Kelly
john.kelly4@nhs.net
07500 225027

4.3 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. Medical information will not normally be required unless it might:

- Help explain the individual understanding of the situation.
- Help explain the individual's propensity for the suspect crime.
- Inform any decision on prosecution.
- Assist the police in carrying out their duties safely.

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.

4.4 Assisting the Police and 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 Local Security Management Specialist and/or Chief Finance Officer.

4.5 Personal Safety & Lone Working

The CCG will develop separate Personal Security and Lone Working guidance. Once published, this document should be referred to by staff for information, guidance and procedures in these areas.

All staff must follow existing Health and Safety policies and guidance.

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

4.6 Premises Security

The Estates and Facilities Departments, in liaison with other Directors and the LSMS, will identify deficiencies in the existing buildings, internal and external areas which affect overall security and programme remedial works to be carried out within a reasonable time-scale. All new construction and modernisation work should include provision of funding for the correct level of security measures.

Security and panic alarms may be installed where appropriate. Advice on systems and locations should be sought from the LSMS, prior to purchasing equipment.

The CCG does not employ any Security Guards at any of it's premises

4.7 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.
- Staff using private vehicles for work must ensure that at no time patient sensitive information is left unattended in vehicles, this includes either in hard paper copy, on laptops or memory sticks
- The security of motor vehicles owned by employees, service users and visitors is the responsibility of the owner of the vehicle.
- All medical equipment transported from the organisation premises for use by clinicians remains the responsibility by either party.
- Equipment must be stored out of sight and under no circumstances should it be left in staff vehicles unattended overnight.
- 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 should not 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 that 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. More details are provided in the CCG Driving at Work Policy.

4.8 IT Security

All staff are required to comply with relevant IT Security Polices. It is the responsibility of individual Directors to ensure that their staff comply with these policies to ensure faith in confidentially between the organisation and its patients, clients and staff

4.9 Identification Badges

ID badges are obtained via the Human Resources Department. These contain information of the card holders name and working department.

All staff should wear their ID badge at all times whilst on CCG premises, or when representing the CCG

Managers must ensure any member of staff, whether permanent or temporary should hand in their ID badge on their last day of employment.

Temporary ID cards/ badges will be issued to all persons undertaking work experience, voluntary work or employed by the CCG.

The loss of an ID badge must be reported immediately to your Manager and the Human Resources Department. An incident form must be completed.

4.10 Cash Movement and Handling

Each department must ensure that they have suitable arrangements in place for the movement of cash/ valuables around the CCG. These arrangements must take into account the security of staff as well as the security of cash/ valuables. Security procedures will also be developed to protect patients/ staff cash or valuables.

4.11 Verbal & Physical Assault or 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.

4.12 Staff Property

Secure storage for staff personal property is provided in a variety of forms. This includes personal lockers in office areas 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 to not bring high value items or large amounts of cash to work with them.

4.13 Lost Property

Property that has been found on the CCG premises should be adequately recorded. Any unclaimed property will be disposed of in accordance with CCG Standing Financial Instructions.

4.14 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 should not 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 should be 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 that they fail safe (i.e. unlocked but closed) in the event of a fire alarm.

Codes for these entry systems are only to be issued to those working in the area, and should never be given to staff not working in that area. Codes should also never be given to patients or visitors and doors with coded entry systems should never be latched or wedged open. Staff should also not just release any electrical entry door without first checking the identity of the person seeking entry. Everyone should also be aware of other persons 'tailgating' 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. Departments should seek the assistance from Estates staff in order to do this.

Departmental keys will remain under the responsibility of the Department and must be accounted for in an orderly system. All keys should 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.

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).

4.15 Closed Circuit Television (CCTV)

Closed circuit television cameras play an important part in crime prevention and

detection in NHS premises. All cameras should 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.

CCTV systems installed in premises used by the CCG will be 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.

4.16 Receipt of Goods

Any member of staff who signs for any goods on behalf of the CCG is accountable for any discrepancies which may occur. All packages delivered must be identified and checked against delivery notes prior signing. 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. The supplies department / stores must be informed. Packages must not be left in a position where they may create a safety/fire risk.

Records must be updated as soon as possible, including any inventory or stock control.

4.17 Suspicious Packages and Telephone Threats

Any suspicious package should **NOT** be moved and its position should be reported to Line Management. Following initial investigation (without touching or moving package) identifying if:-

- 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 should 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 Fire procedure preferably without activating the fire alarm.

Any packages/Letters should not be placed in water, windows should not be opened 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 should be informed immediately, along with the local Director. A decision will be taken by directors as whether an emergency should be declared and whether the CCG's emergency plan is activated.

4.18 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 Castle Point and Rochford CCG. Please familiarise yourself with these.

5.0 COUNTER FRAUD

It is the responsibility of all employees to be alert to the possibility of fraud being perpetrated against the CCG. Procedures should ensure that the Chief Finance Officer and LCFS are alerted immediately of any suspicions of fraud. Fraud costs the NHS some £260 million per year. Fraud can best be defined as obtaining a financial benefit by deceit. Typical examples of fraud against the CCG are as follows:

5.1 Contractors

- Claiming for goods/services not provided.

5.2 Service Users

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

5.3 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 Trust they should contact:

Local Counter Fraud Specialist
eleni.gill@nhs.net
john.kelly4@nhs.net

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

More information on Fraud can be found within the CCG's Fraud, Bribery and Corruption Policy found in the staff intranet.

5.4 Training

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

- All managers and staff need awareness raising training, personal safety awareness and dealing with conflict, as well as preventing and reporting crime in the work place.
- Managers should receive the appropriate advice to ensure that the content of this policy is fully implemented.
- Under the Standard Contract, employers must provide all frontline staff with Conflict Resolution Training. This training should 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.
- All staff will be recalled for half day refresher session within a three year period of initial training.
- Targeted refresher training will be provided for staff when required.

Managers will determine the level of training required by their staff and reassess this training need as and when their roles / job changes. The CCG therefore supports continuous development of systematic training in personal safety.

6.0 POLICY DEVELOPMENT

Consultation and communication with stakeholders during development.

6.1 Approval and ratification process

All non-clinical policies must be formally ratified by the appropriate Board Committee before implementation. This policy will be formally approved by the NHS Castle Point and Rochford CCG board.

6.2 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.

7.0 DISSEMINATION AND IMPLEMENTATION PROCESS, INCLUDING TRAINING

7.1 Dissemination and Implementation

The Chief Finance Officer will ensure that a copy of this policy is freely available to all CCG staff (electronically and/or hard copy).

7.2 Training

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 made available to staff through face-to-face training and e-learning.

All new permanent employees must attend the Induction Programme at the earliest practicable time after commencing employment. This training includes Health, Safety, Welfare, Fire, Security and Back Awareness. 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 an actually attend. Once training needs have been recognised, the managers should then make arrangements for the member of staff to undertake the next available course.

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

8.0 LIBRARY AND ARCHIVING ARRANGEMENTS

The Chief Finance Officer will ensure that the up to date version of the policy is available to all staff, and will archive old versions of the policy.

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

8.1 Monitoring of Compliance and effectiveness

The Chief Finance Officer will ensure that the processes outlined in this policy and any associated policies and guidance are followed. This will be achieved using a Health and Safety compliance tool.

8.2 Associated Documents and Policies

- Lone Workers Policy
- Risk Management Strategy Policy
- Management of Violence & Aggression Policy
- Whistle Blowing Policy
- Management of Incidents Policy and Procedures
- Health and Safety Policy
- Complaints Policy
- IM&T Information Security Policy
- Fire Safety Policy

8.3 References and Definitions

References

- Health and Safety at Work etc. 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”)

9.0 EQUALITY IMPACT ASSESSMENT

NHS Castle Point and Rochford CCG is committed to carrying out a systematic review of all its existing and proposed policies to determine whether there are any equality implications.

This policy has been assessed using NHS Castle Point and Rochford CCG ’s Equality Impact Assessment and identified as having the following impact upon equality and diversity issues.

Age	Disability	Gender	Race	Sexuality	Religion	Human Rights	Total Points	Impact
0	0	0	0	0	0	0	0	Low

10.0 LIST OF STAKEHOLDERS CONSULTED

Name	Title	Comments received Y/N	Comments incorporated Y/N
Members of the CCG's Senior Management Team	19.08.2016	APPROVED	N
Governing Body	04.08.2016	APPROVED	N

11.0 VERSION CONTROL SHEET

Version	**Date Issued**	**Date of next review**	**Author Name and Title**	**Comment**
001	October 2014	October 2015	Local Security Management Specialist	Presented to Audit and Risk Committee on 13th November 2014
002	July 2016	July 2018	Local Security Management Specialist	
003	November 2019	November 2021	Local Security Management Specialist	