# SECURITY MANAGEMENT POLICY

<table>
<thead>
<tr>
<th>Policy Author(s)</th>
<th>Health &amp; Safety Team, Midlands &amp; Lancashire CSU</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accountable Manager(s)</td>
<td>Jan Snoddon, Chief Nurse</td>
</tr>
<tr>
<td>Ratified by (Committee/Group)</td>
<td>Integrated Governance Committee</td>
</tr>
<tr>
<td>Date Ratified</td>
<td>30th November 2016</td>
</tr>
<tr>
<td>Target Audience</td>
<td>All staff, including temporary staff and contractors, working for or on behalf of NHS Halton CCG</td>
</tr>
<tr>
<td>Review Date</td>
<td>November 2017</td>
</tr>
</tbody>
</table>

This Policy has been developed by Midlands & Lancashire Commissioning support Unit (CSU).

This policy has been approved and adopted by NHS Halton CCG and are applicable to all staff, including contractors and volunteers.

## VERSION HISTORY

<table>
<thead>
<tr>
<th>Issue Date</th>
<th>Version No</th>
<th>Brief Description of Change</th>
<th>Changed by</th>
</tr>
</thead>
<tbody>
<tr>
<td>30/11/16</td>
<td>1</td>
<td>N/A – New Policy</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Security Management Policy and Strategy

Author/s: Andy Collins

In Consultation with: NHS Halton CCG

Formally ratified/approved by: Integrated Governance Committee (IGC)

Sphere of Activity: Corporate Governance

Version Number: 1

Date of previous revisions: -

Distribution: NHS Halton CCG Intranet

Target Audience: All staff

POLICY STATEMENT / KEY OBJECTIVES

NHS Halton CCG recognises and will ensure that all reasonably practicable measures are taken to deliver a properly secure environment for all who work and visit NHS Halton CCG premises and/or other places of work.

REFERENCES AND SUPPORTING DOCUMENTS

NHS Protect Standards for Commissioner 2016/17

<table>
<thead>
<tr>
<th>Date Stage 1 of Equality Impact Assessment was carried out:</th>
<th>10/02/16</th>
</tr>
</thead>
<tbody>
<tr>
<td>Was a Stage 2 Equality Impact Assessment Carried out?</td>
<td>n/a</td>
</tr>
<tr>
<td>Date Stage 2 of Equality Impact Assessment was undertaken:</td>
<td>n/a</td>
</tr>
<tr>
<td>Date sent for ratification</td>
<td>30/11/16</td>
</tr>
<tr>
<td>Date published on the Website</td>
<td>08/02/17</td>
</tr>
</tbody>
</table>
## Contents

1. Introduction .................................................................................................................. 4
2. Purpose ......................................................................................................................... 4
3. Strategy ......................................................................................................................... 5
4. Scope ............................................................................................................................. 6
5. Definitions ..................................................................................................................... 7
6. Roles and Responsibilities ............................................................................................ 7
7. Risk Management ......................................................................................................... 11
8. Reporting and Review of Security Incidents and Lessons Learnt ................................. 13
9. Security Management Awareness ............................................................................... 14
10. Monitor and Review of Policy .................................................................................. 14
11. References & Bibliography ....................................................................................... 15
12. Related Policies .......................................................................................................... 15
1. Introduction

NHS Halton CCG recognises and will ensure that all reasonably practicable measures are taken to deliver a proper secure environment for all who work and visit Halton CCG’S premises and/or other places of work.

This document has been written in line with NHS Protect’s ‘Standards for Commissioners’, setting out key responsibilities for Clinical Commissioning Groups, for its staff and for those services it commissions under the NHS Standards Business Contract, Service Condition 24.

It defines the main functions and responsibilities of those involved in implementing this policy. This document will be available to all employees and providers via the CCG website. It should be read carefully and its guiding principles adhered to.

2. Purpose

The purpose of this strategy and policy is to detail NHS Halton CCG’s aims and 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.

The CCG will develop a culture which recognises the importance of security;

- Provide and maintain a working environment that is safe and free from the danger of crime for all people who may be affected by its activities including employees, patients and visitors.
- Prevent loss of/or damage to CCG assets or property as a result of crime, malicious acts, loss, damage or trespass.
- Maintain good order of premises under CCG control.
- Report all criminal activity to CCG management and ensure a robust response in line with national NHS Protect guidance.
- Provide support to staff involved in a security incident and supply up to date information for all parties, especially after an incident.
- Work in partnership with local agencies e.g. police and local authority to ensure a safe and secure environment within all NHS Halton CCG locations.
- Support all staff who have been a victim of assault (both physical and verbal), through the course of their work, supporting civil prosecution where the Crown Prosecution Service (CPS) will not pursue this.
- Build the internal and external profile of Halton CCG as an organisation that takes security seriously, from prevention of crime through to prosecution of those committing crime against it.
3. **Strategy**

NHS Halton CCG’S anti-crime strategy sets out its aims to continuously improve its anti-crime provision to safeguard the CCG for the future. In order to ensure this continuous improvement, aligned with NHS Protects NHS Anti-Crime Strategy, there are four strategic aims:

- To provide **leadership** for all NHS Halton CCG’S crime work by applying an approach that is strategic, co-ordinated, intelligence-led and evidence based.

- To **work in partnership** with NHS Protect, other NHS commissioners and providers, as well as key stakeholders, such as the Police, the Crown Prosecution Service and local authorities.

- To **establish a safe and secure environment** that has systems and policies in place to: protect NHS staff from violence, harassment and abuse; safeguard NHS property and assets from theft, misappropriation or criminal damage.

- To lead, within a clear professional and ethical framework, **investigations** into losses due to criminality and criminal behaviour towards Halton CCG’S staff.

These aims will be met by working in accordance with the following three key principles, which underpin all anti-crime work in the NHS.

**Inform and Involve**

- NHS Halton CCG’S communicates with other bodies, including providers, regulators and advisory bodies regarding security issues, including violence, theft and criminal damage.

- NHS Halton CCG’S carries out risk assessments to identify risks within the organisation relating to the security of its staff, property, premises and assets.

- NHS Halton CCG’S will develop proportionate and effective policies to mitigate identified risks.

- NHS Halton CCG’S will evidence communication between relevant departments within its organisation, on security matters.
Prevent and Deter

- NHS Halton CCG’S risk assess job roles and undertakes training needs analysis for all employees, contractors and volunteers whose work brings them into contact with NHS patients and members of the public. As a result, training provided will be in accordance with NHS Protects guidance on conflict resolution training. The training is monitored, reviewed and evaluated.

- NHS Halton CCG’S assess risks to lone workers, including the risk of violence. HALTON CCG’S will take necessary steps to avoid or control the risks and these measures are regularly and soundly monitored, reviewed and evaluated for their effectiveness.

- NHS Halton CCG’S distributes national and regional NHS Protect alerts to primary care contractors, relevant staff and third parties, taking action to raise awareness of security risks and incidents. This process will control, monitor, review and be evaluated.

Hold to Account

- NHS Halton CCG’S has arrangements in place to ensure that security related incidents are investigated in a timely and proportionate manner and these arrangements are monitored, reviewed and evaluated.

- NHS Halton CCG’S is committed to applying all appropriate sanctions against those responsible for security related incidents.

4. Scope

4.1 This Policy applies to all directorates, services and departments of NHS Halton CCG including contracted or embedded staff and in all aspects of its activities.

4.2 This Policy covers the security of staff, contractors, visitors and property within. It focuses on improving and sustaining physical and personal security.

4.3 NHS Halton CCG Security Policy is based on the framework recommended as best practise by NHS Protect, which its aim is to:

To protect the NHS so that it can better protect the public’s health.
5. Definitions

5.1 NHS Protect

Is the strategic body of the NHS to guide all NHS organisations to tackle security related issues and provide direction on these matters.

5.2 Physical Assault

The intentional application of force to the person, without lawful justification, resulting in physical injury or personal discomfort.

5.3 Non-Physical Assault

The use of inappropriate words or behaviour causing distress and/or constituting harassment.

6. Roles and Responsibilities

6.1 NHS Halton CCG Senior Executive team acknowledge its responsibilities for security management as employers and commissioners by following NHS Protects ‘Standards for Commissioners’. This set of standards will be followed by the CCG and a self-assessment will assess compliance, which may result in an audit from NHS Protect Senior Compliance and Quality Inspectors.

6.2 Clinical Chief Officer

The Clinical Chief Officer has appointed the Head of Corporate Business as the Security Management Director (SMD), having the responsibility for raising the profile of security management work within the organisation and Governing Body level, gaining their support and backing for important security management strategies and initiatives.

6.3 Security Management Director (SMD) takes overall responsibility for all aspects of operational security matters, ensuring the following are considered:

- Appropriate policies are developed.
- Arrangements and appropriate levels of provision are in place for security management to take place effectively. This should be reviewed annually;
- Ensuring reports and returns are made to NHS Protect.
- Serious incidents and criminal acts are reported internally and investigated.
- Working with the police and/or Local Security Management Specialist (LSMS) in seeking prosecution of perpetrators of criminal acts, violent behaviour and verbal abuse.
- Providing feedback to staff involved in the more serious incidents.
- Ensure security management objectives are discussed and reviewed at a strategic level within the organisation.
- Ensure strategic management and support of security management work within the organisation, and leads on seeking assurance from providers regarding their compliance with security management requirements through contract monitoring processes. (NHS Standards Contract, service condition 24).
• Ensures assurance is actively sought from providers and measures are in place to ensure this takes place regularly.

6.4 Directors – It is the responsibility of all Directors to:
• Disseminate the Security Management Policy within the area of their responsibility.
• Ensure the co-ordination of security issues with other employers who share the worksite with the CCG.
• Ensure the implementation of the Security Management Policy within the area of their responsibility by providing support and advice to their managers.

6.5 Local Security Management Specialist (LSMS)

The nominated Local Security Management Specialists (LSMS) will provide professional skills and expertise to tackle security management issues on behalf of the CCG.

The overall objective of the LSMS will be to work on behalf of the CCG to deliver an environment that is safe and secure for all staff to the highest standards.

The LSMS will:
• Prepare a written work plan, with SMD and prepare annual reports on progress against the plan.
• Complete Commissioners Self Review tool, in conjunction with the CCG, and submit to NHS Protect annually.
• Provide advice and support to the CCG on all security matters.
• Be responsible for advising on the security of all the locations within the CCG, carry out inspections, write reports and advise the CCG on all matters of security.
• Work closely with NHS Protect and respond to all initiatives and disseminate security alerts to the CCG.
• Provide advice to managers at all levels on security matters/measures and deal with the management of violent and aggressive behaviour.
• Provide assistance to managers implementing risk reduction measures and post-incident management.
• Report the results of Security Surveys/Risk Assessments undertaken to the appropriate Manager and SMD.
• Assist local managers in carrying out investigations into security related incidents, liaising as required with the Police, NHS Protect, Legal Protection Unit and assisting in evidence gathering for submission to Court as part of the prosecution process.
• Deliver awareness sessions to staff on this Policy and to create a Pro-security Culture within the CCG.
• To foster links with local agencies and bodies, such as the Police, Crime Disorder Partnerships and other security professionals in Neighbouring organisations.
• Provide advice, guidance and assistance to managers undertaking security risk assessments.
6.6 Managers

It is the individual manager’s responsibility to ensure that safe and secure environments are maintained, that all incidents are reported in full and that appropriate action is taken when and where necessary. Security is the responsibility of all managers who must ensure that preventative measures for the safety of staff and property are in place. They should ensure that the right policies, procedures and systems are in place in their local areas and that such policies are kept under constant review.

Line managers and department heads should also:

- Ensure that arrangements are made to secure the Department/Directorate out of working hours, together with the safe custody of keys.
- Ensure the setting of any security alarm or device to protect the property out of hours.
- Seek advice from the LSMS to ensure that the highest standard of security is maintained within their Department/Directorate.
- Ensure all staff employed by the CCG, staff from other organisations working in NHS Midlands & Lancashire CSU (MLCSU), contractors and official visitors wear an ID badge at all times.
- Ensure that all staff are made aware of this Security Policy and fully understand its content and their responsibilities.
- Assess the impact on security of new projects and changes.
- To carry out security risk assessments and ensure that appropriate measures are in place.
- Ensure all staff receive appropriate security training by means of a training needs analysis and risk assessment for their role.

6.7 CCG Employees

- CCG employees are expected to co-operate with management to achieve the aims, objectives and principles of the Security Management Policy. Great emphasis is placed on the importance of co-operation of all staff playing their part in observing security and combating crime.

- CCG employees have a number of duties and responsibilities regarding security, these include.

- Staff should ensure they keep property and assets of the CCG secure at all times. Loss of equipment supplied by the CCG may be investigated by LSMS and not replaced. Staff may have to fund replacement equipment, through their own department budget, should they lose or damage through negligence, any property or assets of the CCG.

- Staff should be aware of their responsibilities in protecting at all times, the assets/property of contractors, visitors and the CCG. Where specific security procedures exist, staff must abide by them at all times. Where staff know or suspect a breach in security, they must report it immediately on an Incident Form or to their manager, or LSMS.

- All staff are reminded that it is a criminal offence to remove property belonging to the CCG without written authority. Failure to seek appropriate authority from
their line manager could result in disciplinary action or criminal proceedings being taken against them.

- Staff are responsible at all times, for the protection and safe keeping of their private property. The LSMS will, if requested, advise staff on the security of their property. Any loss of private property must be reported without delay. If private property has been stolen, then it is the owner’s responsibility, not the CCG’s responsibility, to contact the police. Theft will be seen as from the person not the CCG by the Police.

- The CCG will not accept liability for the loss of, or damage to private property including motor vehicles or other modes of transport. Motor vehicles brought onto the CCG’s car parking facilities are entirely at the owner’s risk.

- All staff, visitors and contractors working on behalf of the CCG or its representative, must wear an approved security identification badge and/or pass at all times, and challenge colleagues or strangers for not wearing them.

- Should a member of staff be vulnerable for any reason, or have a disability that could impact upon their security needs, they should bring this to the attention of their line manager who will make the necessary arrangements for drawing up a Personal Security Plan if required.

- Report all security related incidents, including violence and aggression, theft or loss through the CCG incident reporting procedures, ensuring that line managers are fully aware of the circumstances.

- Be aware of security issues at all times and not allow anyone to tailgate them through controlled access doors. All staff must use their tobs to gain access through all doors at all times.

6.8 Staff from Other Organisations

Staff from other organisations e.g. Midlands and Lancashire CSU, should be made aware and read the details of the CCG’s Security Management Policy. Where required, the CCG will ensure adequate liaison is established between other bodies to ensure consistency of procedures and guidelines.

CCG staff visiting or working at other organisations should familiarise themselves with security arrangements for that location and if necessary, risk assess any perceived risks outlined in this policy.

6.9 NHS Protect

NHS Protect leads on work to identify and tackle crime across the health service. The aim is to protect NHS staff and resources from activities that would otherwise undermine their effectiveness and their ability to meet the needs of patients and professionals. Ultimately, this helps to ensure the proper use of valuable NHS resources and a safer, more secure environment in which to deliver and receive care.
NHS Protect has five high-level organisational aims. These are:

- To provide national leadership for all NHS anti-crime work by applying an approach that is strategic, co-ordinated, intelligence-led and evidence based.

- To work in partnership with the Department of Health, commissioners and providers, as well as our key stakeholders, such as the Police, CPS and local authorities to coordinate the delivery of our work, and to take action against those who commit offences against the NHS.

- To establish a safe and secure physical environment that has systems and policies in place to protect NHS staff from violence, harassment and abuse; safeguard NHS property and assets from theft, misappropriation, or criminal damage; and protect resources from fraud, bribery and corruption.

- To lead, within a clear professional and ethical framework, investigations into serious, organised and/or complex financial irregularities and losses which give rise to suspicions of fraud, bribery or corruption.

- To quality assure the delivery of anti-crime work with stakeholders to ensure the highest standard is consistently applied.

From 1 February 2016, NHS Protect will become a 'prescribed person' under the Public Interest Disclosure Act 1998 (PIDA), which provides the statutory framework for protecting workers from harm if they blow the whistle on their employer.

7. Risk Management

NHS Halton CCG risk management policy should be followed and can be found on the CCG website.

NHS Halton CCG has identified the following potential security related risks for its organisation:

- Physical Assault against staff
- Non-Physical Assault against staff
- Harassment of staff by another
- Theft of CCG property
- Theft of personal belongings
- Criminal damage
- Unauthorised intruders

A risk assessment will be completed following the CCG’s Risk Management Policy to analyse the impact and likelihood of those potential risks, and escalate any that meet the threshold for a corporate risk register. Risk assessments have been included in this policy in appendix one.
7.1 Managing Physical Security

The following steps should be taken annually to ensure the management of physical security is maximised at all times:

- A site wide risk assessment of all physical security in place at all buildings under the control of the CCG in accordance with the CCG Risk Management Strategy.
- An assessment must take place to improve or increase security after an incident or new vulnerabilities realised by the CCG and Security Management Director.

7.2 Visitors/Contractors

- Contractors and other personnel, who visit the CCG, are to be issued with a visitor’s identification badge that must be displayed at all times when personnel are on the premises.
- This will be signed for in the register held at the appropriate reception area. The member of staff who is responsible for the visitor/contractor will then arrange for them to be escorted to the relevant department.
- On leaving, the visitor’s badge should be reclaimed. All relevant times should be recorded in the register held within the department.

7.3 Staff Identification

The CCG Security Management Policy requires that all staff wear identification badges at all times. Photographic identification badges for staff will be produced by the Midlands and Lancashire CSU and issued via your line manager.

7.4 CCTV

The installation of CCTV at sites identified as benefiting from the facility is for the primary purpose of deterring criminal activity against the CCG, its staff or visitors. An annual review of CCTV need or requirements will take place following an incident or identified vulnerabilities were it is deemed necessary to strengthen the security of the CCG and its staff.

- Where crime is committed any relevant data captured by CCTV will be used as evidence to support criminal or civil prosecution of the perpetrator/s. This may include the use of third parties data e.g. Landlords CCTV.
- Access to images will be governed in accordance with ICO guidelines (in accordance with the Data Protection Act, Section 29) and Subject Access Requests.

7.5 Access Control and Fobs

CCG staff will be issued with a fob for access to the buildings and areas they are employed to work within.

- Fobs will only be issued to employed staff (including those working as embedded or at the discretion of the Security Management Director) or visitors who have
business at CCG and have signed for their use. Visitor fobs must be returned at the end of each day.

- Data in relation to the activity of fobs will be recorded by the access control computer and this data may be used in the prevention or detection of crime, in accordance with the Data Protection Act, Section 29 and Subject Access Requests. It must not be misused for any reason.

- It may also be used for a fire register should the need arise during a drill or fire situation. All staff are therefore required to present their fobs on entry and exit of the main building regardless of the position of the main doors.

**Loss of CCG Equipment/Assets**

The CCG will provide staff with equipment e.g. iPads and laptops, for staff members to conduct their work. Staff must take care of equipment and ensure it is secure at all times. Staff must take care when off site and travelling to another meeting or venue, with CCG equipment/assets.

Staff who are deemed to have acted carelessly with CCG equipment/assets may be subject to disciplinary proceedings.

Should a department want to replace this item then replacement would be at the discretion of the Security Management Director and may have to be funded out of that department’s budget.

8. **Reporting and Review of Security Incidents and Lessons Learnt**

- The CCG should follow its own incident reporting procedures to report security related incidents.

- The LSMS should review all security incidents; including security related Serious Incidents and report to the Security Management Director on steps required following LSMS findings.

- The LSMS will report all security incidents to NHS Protect’s SIRS (Serious Reporting Incident System), held by NHS Protect, to provide a national picture for security across the whole of the NHS.

- Lessons learnt from security management related incidents will be reported to the Integrated Governance Committee for review and implementation.
9. Security Management Awareness

- The LSMS will attend staff training sessions to raise awareness of Security Management within the CCG.

- Additional training will be based on training needs analysis e.g. Conflict Resolution training.

10. Monitor and Review of Policy

The outcome of the successful implementation of the Security Management Policy will be reviewed at the Integrated Governance Committee. The Committee will review the security related incidents, security related risk assessments and statistical analysis of security reports given to the group.

This policy will be reviewed annually by the Integrated Governance Committee at its first meeting in the financial year and in accordance with the following as and when required:

- Following legislative changes
- Publication of good practice guidance
- Case law
- Significant incidents reported
- New vulnerabilities identified
- Changes to organisational infrastructure
11. References & Bibliography

Directions to NHS Bodies on Security Management Measures 2004

NHS Protects Standards for Commissioners 2016/17

Concordat between Health and Safety Executive & CFSMS

Memorandum of Understanding between the Associations of Chief Police Officers (ACPO) and the NHS Security Management Service

CCTV Code of Practice

12. Related Policies

The following documents should be consulted alongside this policy:

- Management of Violence and Aggression Policy
- Lone Working Policy
- Statutory and Mandatory Training Policy
- Incident Reporting Procedure
- Risk Management Strategy