18 AC
Security Strategy and Policy

<table>
<thead>
<tr>
<th>Policy number</th>
<th>18 AC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>1.1</td>
</tr>
<tr>
<td>Approved by</td>
<td>Audit Committee</td>
</tr>
<tr>
<td>Name of author/originator</td>
<td>Andy Kelly, Estates and Facilities Manager</td>
</tr>
<tr>
<td>Owner (director)</td>
<td>Elaine Newton, Director of Governance and Compliance</td>
</tr>
<tr>
<td>Date of approval</td>
<td>March 2017</td>
</tr>
<tr>
<td>Date of last review</td>
<td>March 2015</td>
</tr>
<tr>
<td>Review to be completed by</td>
<td>March 2019</td>
</tr>
<tr>
<td>Version</td>
<td>Date</td>
</tr>
<tr>
<td>---------</td>
<td>--------------</td>
</tr>
<tr>
<td>1.0</td>
<td>February 2017</td>
</tr>
<tr>
<td>1.1</td>
<td>March 2017</td>
</tr>
</tbody>
</table>
Equality statement

NHS Guildford and Waverley aims to design and implement services, policies and measures that meet the diverse needs of our service, population and workforce, ensuring that none are placed at a disadvantage over others. We take into account the Human Rights Act 1998 and promote equal opportunities for all. This document has been assessed to ensure that no employee receives less favourable treatment on the protected characteristics of their age, disability, sex (gender), gender reassignment, sexual orientation, marriage and civil partnership, race, religion or belief, pregnancy and maternity.

Members of staff, volunteers or members of the public may request assistance with this policy if they have particular needs. If the member of staff has language difficulties and difficulty in understanding this policy, the use of an interpreter will be considered.

We embrace the four staff pledges in the NHS Constitution. This policy is consistent with these pledges.

See next page for an Equality Analysis of this policy.
Equality Analysis

Equality analysis is a way of considering the effect on different groups protected from discrimination by the Equality Act, such as people of different ages. There are two reasons for this:

- to consider if there are any unintended consequences for some groups
- to consider if the policy will be fully effective for all target groups

<table>
<thead>
<tr>
<th>Name of Policy:</th>
<th>Policy Ref:</th>
<th>Is this New? [ ] Or Existing? [X ]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Strategy and Policy</td>
<td>18 AC</td>
<td></td>
</tr>
</tbody>
</table>

**Assessment conducted by (name, role):**
Andy Kelly, Estates and Facilities Manager

**Date of Analysis:**
27/10/2016

**Directorate:**
Governance and Compliance
**Director's signature:**

Who is intended to **follow** this policy? Explain the aim of the policy as applied to this group.
All Guildford & Waverley Staff, visitors and contractors.
To ensure a secure and safe working environment at all times

Who is intended to **benefit from** this policy? Explain the aim of the policy as applied to this group.
All Guildford & Waverley Staff, visitors and contractors.
To ensure a secure and safe working environment at all times

1. **Evidence considered.**
   Security risk assessment as carried out and provided by TIAA

2. **Consultation.** *Have you consulted people from protected groups? What were their views?*
   N/A

3. **Promoting equality.**
   Yes. As it looks to ensure that all groups within the building are safe and secure at all times.

4. **Identifying the adverse impact of policies**
   None identified

a) **People from different age groups:**
   No adverse impact predicted from this policy

b) **Disabled people:**
   Lift in Place and use of an evac chair
c) **Women and men:**
   - No adverse impact predicted from this policy

d) **Religious people or those with strongly held philosophical beliefs:**
   - No adverse impact predicted from this policy

e) **Black and minority ethnic (BME) people:**
   - No adverse impact predicted from this policy

f) **Transgender people:**
   - No adverse impact predicted from this policy

g) **Lesbians, gay men and bisexual people:**
   - No adverse impact predicted from this policy

h) **Women who are pregnant or on maternity leave:**
   - No adverse impact predicted from this policy

i) **People who are married or in a civil partnership:**
   - No adverse impact predicted from this policy

<table>
<thead>
<tr>
<th>5. Monitoring</th>
<th>How will you monitor the impact of the policy on protected groups?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Through the Staff Partnership Forum `</td>
</tr>
</tbody>
</table>
# Contents

Equality statement ............................................................................................................. 3
Equality Analysis ................................................................................................................... 4

1.0 Introduction of Strategy and Policy Objective ................................................................. 9
1.1 Introduction ...................................................................................................................... 9
1.2 Aim ................................................................................................................................ 9
1.3 Objectives ........................................................................................................................ 10
1.4 Anti-crime strategy and approach .................................................................................. 10
1.5. Key principles ................................................................................................................ 11
1.6. Business process ............................................................................................................ 11

2.0 Legislative Framework/Core Standards .......................................................................... 13

3.0 Scope ............................................................................................................................... 13
3.1 Holistic Approach ........................................................................................................... 13

4.0 Definitions ....................................................................................................................... 13

5.0 Roles and Responsibilities ............................................................................................ 15
6.0 Procedure ........................................................................................................................ 18
6.1 G&W CCG Security Priority ......................................................................................... 18
6.2 Risk Management .......................................................................................................... 18
6.3 Incident Reporting ......................................................................................................... 19
6.4 Access Controls ............................................................................................................. 19
6.5 Identification .................................................................................................................. 19
6.6 Training ........................................................................................................................... 19
6.7 Security Measures ......................................................................................................... 19
6.8 Monitoring ...................................................................................................................... 21
6.9. Sanctions and Recovery ............................................................................................... 21
6.10 Premises and Asset Security Guidelines ..................................................................... 21
6.11. Building Security ....................................................................................................... 21
6.15. Visitors and Contract staff ......................................................................................... 23
6.16. Asset security ............................................................................................................. 24
7. CCTV Policy ................................................................................................................. 25
  7.1. Introduction ............................................................................................................... 25
  7.2. Purpose, Aims and objectives .................................................................................. 26
  7.3. Purpose of the system .............................................................................................. 26
  7.4. Roles and Responsibilities ...................................................................................... 27
  7.5. CCTV system ........................................................................................................... 28
  7.6. Access to images ..................................................................................................... 30
  7.7. Documentation ......................................................................................................... 30
  7.8 Standard Operating Procedures CCTV ................................................................. 30

8.0 Procedure for dealing with bomb threats, suspect packages and other threats
  8.1. Introduction ............................................................................................................... 32
  8.2. Purpose, aims and objectives .................................................................................. 32
  8.3. Roles and Responsibilities ...................................................................................... 33
  8.4. General Guidelines ................................................................................................. 34
  8.5. The Threat ............................................................................................................... 34
  8.6. Actions to be taken by person receiving the call .................................................... 34
  8.7. Reporting the incident ............................................................................................ 35
  8.8. Threats received by other means ............................................................................ 35
  8.9. Discovery of Suspect Packages ............................................................................. 36
  8.10. Car Bombs ............................................................................................................ 36
  8.11. Return area to all Clear/Stand down .................................................................... 36
  8.12. Debrief .................................................................................................................. 36
  8.13. Bomb Threat and the Law ..................................................................................... 36
  8.15. Chemical / Biological Material. ............................................................................ 38
  8.16. Dealing with the Media ......................................................................................... 38
  8.17. Staff Training ......................................................................................................... 38
  8.18. Post-Incident Review ............................................................................................. 38

9. Lockdown Policy .......................................................................................................... 39
  9.1. Introduction ............................................................................................................... 39
  9.2. Purpose, aims and objectives .................................................................................. 39
  9.3. Limitations in a lock down ...................................................................................... 39
  9.4. Planning a lock down ............................................................................................... 40
  9.5. Levels of lock down ................................................................................................ 40
9.6. Declaration of a G&W CCG lock down ................................................................. 41
9.7. Initiation of lock down procedures ................................................................. 41
9.8. Command and control ................................................................................... 41
9.9. Stand down .................................................................................................... 41
9.10. Training ....................................................................................................... 42
10 References ....................................................................................................... 42
11 Appendix 1 Procedural Document Checklist for Approval ......................... 43
12 Appendix 2 Compliance & Audit Table ............................................................. 45
1.0 Introduction of Strategy and Policy Objective

1.1 Introduction

NHS Guildford and Waverley CCG aims to commission the best possible health care available to its patients. Crime against the NHS undermines its effectiveness and ability to deliver healthcare. Crime diverts resources from their proper use, patient care, and has far-reaching effects on the ability of the NHS to meet the needs of the public.

This Policy brings together a number of security areas into one Policy, with separate sections detailing the specific responsibilities that apply, in order to meet statutory requirements.

There are many types of crime that could affect the NHS, including the following areas:
- violence
- counter terrorism security preparedness
- criminal damage
- theft
- bribery
- corruption fraud
- unlawful action (market fixing etc).

The CCG is committed to providing a ‘caring, secure, and supportive’ environment to all who interact with the organisation. It recognises that it has a clear and overarching ‘duty of care’ to ensure that all reasonable security control measures are present to support the principles of a ‘safe and secure’ environment, providing optimum opportunity for staff to deliver the best possible service. In order to achieve these objectives, it is a fundamental requirement that all persons feel confident of the security service and the security measures in place. Furthermore all staff and visitors must recognise that they have a duty to support the security function at all times. In accordance with these objectives any security breach or crime occurrence can seriously undermine the CCG objectives with a significant adverse impact on the organisation and its staff.

This policy also supports compliance with frameworks against which the CCG is assessed, including compliance with the Care Quality Commissions.

1.2 Aim

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

- The protection, safety, security and welfare of staff, patients, visitors, contractors and all who attend CCG premises
- The provision of efficient and effective security control measures to minimise criminal activity including incidents of violence and aggression, loss, damage and/or theft of CCG property and assets
• Minimising disruption to or loss of service to patients and staff.
• Prevent crime by targeting and co-ordinating work effectively, building in anti-crime measures at all stages of local policy development, and reflecting wider government initiatives where appropriate.
• Be compliant with the NHS Standard Contract, and take into account the draft commissioner standards for Security. These standards provide a more detailed framework of requirements that apply to commissioner organisations.

1.3 Objectives

This process will ensure that adequate security measures are present with the primary objectives of:

• Ensuring that security surveys and risk assessments are carried out on the CCG premises and departments to identify any security risks and recommend measures that are proportionate and commensurate with the risks highlighted
• The adequate monitoring of such risk assessments to ensure compliance
• The provision of a secure environment for staff and all who interact with the organisation and, without prejudice to the interest of the organisation, their personal property
• Regular liaison with the Police (both local and national levels), other relevant law enforcement and regulatory agencies (e.g. Environment Agency) and NHS Protect to identify security and crime risk trends
• As appropriate, providing support and assistance to staff, patients and visitors who have being subject of a criminal act or exposed to an untoward security related incident.

The purpose of this policy is to also implement the specific requirements of NHS Protect.

1.4 Anti-crime strategy and approach

The CCG's security strategy reflects the anti-crime strategy and approach as stated by NHS Protect.

• Applying an approach that is strategic, co-ordinated, intelligence led and evidence based.
• Working in partnership, where needed or required, with the Department of Health, commissioners and other providers, as well as key stakeholders, such as the police, the CPS, local authorities and professional organisations such as the National Fraud Authority and the Cabinet Office Counter Fraud Task Force, to coordinate the delivery of security management work and to take action against those who commit offences against the NHS.
• Establishing 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; and protect resources from fraud, bribery and corruption.
• Leading, 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.

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

1.5. Key principles

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

• **Inform and Involve** those who work for or use the NHS about crime and how to tackle it. NHS staff and the public are informed and involved with a view to increase understanding of the impact of crime against the NHS.

• **Prevent and Deter** crime in the NHS to take away the opportunity for crime to occur or to re-occur and discourage those individuals who may be tempted to commit crime, by implementing robust systems, which will be put in place in line with policy, standards and guidance developed by NHS Protect. Successes may be publicised so that the risk and consequences of detection are clear to potential offenders.

• **Hold to account** those who have committed crime against the NHS. Crimes must be detected and investigated, suspects prosecuted where appropriate, and redress sought where possible. Where necessary and appropriate, this work will be conducted in partnership with the police and other crime prevention agencies. In relation to economic crime, investigation and prosecution will take place locally wherever possible. NHS Protect will deal with cases which are complex or of national significance through the National Investigation Service. Where recovery of monies lost to crime is viable, this will be pursued. In relation to crimes against NHS staff, criminal damage or theft against NHS property, investigation and prosecution will be undertaken in liaison with the police and CPS or where necessary NHS Protect.

1.6. Business process

The Process Chart brings together the collection of information and intelligence from a number of potential sources, enabling a strategic assessment to inform organisational priorities and resulting actions to deliver the necessary outputs.
Process Chart

- Tasked Information
- Routine Data
- Organisational Feedback

Information is collected, analysed and evaluated

Priorities

Principles for Action

Outputs
- Inform & Involve
- Prevent & Deter
- Hold to Account
2.0 Legislative Framework/Core Standards

This policy is based on the framework policy recommended by NHS Protect. The policy sets out the CCG’s statutory and mandatory responsibilities in respect of a number of directives and monitoring bodies, including the NHS Security Management Service, Health and Safety Executive, Health and Safety at Work Act 1974, Management of Health and Safety at Work Regulations 1999, Healthcare Commission and NHS Litigation Authority. The policy also includes detailed information on security management priority areas and auditable standards/key performance indicators.

3.0 Scope

The Scope of this policy includes:

• Staff personal safety and the personal safety of those who interact with the organisation

• The security of staff premises and assets (owned or leased).

This policy describes the organisational structures, arrangements and responsibilities of staff for the management of Security within the CCG in order to ensure compliance with the NHS Security Management Service’s recommendations.

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

3.1 Holistic Approach

The CCG aims to take a holistic approach to security management, where all security aspects of the different services are considered.

Therefore security management is part of all relevant policies and procedures, and it is advised that the security management strategy is read in conjunction with policies relating to:

• Internet & Email Access and Security
• Information Management And Technology Policy
• Lone Workers Policy
• Lock down procedures
• Emergency Planning
• Business Continuity
• Information Governance
• Accident/Incident Reporting
• Risk Management Strategy/Policy

4.0 Definitions

• NHS Protect: is the working name for the Counter Fraud and Security Management Service (CFSMS): This organisation has responsibility for all policy
and operational matters relating to the prevention, detection and investigation of fraud and corruption and the management of security in the National Health Service.

- **Lockdown**: Lockdown is the process of preventing freedom of entry, exit and movement around a CCG site or other specific building / area, in response to an identified risk, threat or hazard that might impact upon the security of patient, staff or indeed the capacity of that facility to continue to operate.

- **Malicious acts**: Deliberately behaving in a way that is likely to upset or hurt someone.

- **Physical Security**: This term is understood by Health & Safety professionals relates to buildings and objects as any security hardware including locks, access control, intruder alarms, panic alarms, barriers etc that supports the security function.

- **Security**: A state of being where the risks to people and property are minimised in relation to any actions that may lead to personal injury, threat to life or the disruption of business activity of the organisation.

- **Trespass**: To go onto someone’s private property without their permission

- **Security Incident**: Any act or omission that has the potential to undermine the integrity of the CCG’s Security objectives and would include non-compliance whether deliberate or otherwise with the CCG Security Policy and/or local security arrangements.

- **Criminal Act**: Any violation or attempted violation of law whether statute or common law and would include such offences that are more likely to occur within the healthcare setting such as:
  - Harassment
  - Assaults and threats of violence
  - Theft and kindred offences such as burglary
  - Criminal Damage
  - Offences relating to Public disorder
  - Fraud.

- **Premises**: The physical buildings, grounds and all property contained within the CCG boundaries in which NHS staff and professionals work and from which the business of the NHS is delivered.

- **Assets**: Irrespective of their value, ‘Assets’ can be defined as the materials and equipment used directly or indirectly to deliver NHS healthcare. In respect of staff, professionals and patients, the definition can also apply to their personal possessions they retain whilst on CCG premises or working in or providing a service to the NHS.

- **Lockdown**: is the process of controlling the movement and access – both entry and exit – of people (NHS staff, patients and visitors) around the CCG site or other specific CCG building/area in response to an identified risk, threat or hazard that might impact upon the security of patients, staff and assets or indeed the capacity of that facility to continue to operate. A lockdown is achieved through combination of physical security measures and the deployment of security personnel.


- **NHS Security Management Service – Preparing a Lockdown for your CCG**

- **Secured by Design - CCGs (April 2005)**
### 5.0 Roles and Responsibilities

<table>
<thead>
<tr>
<th>Party</th>
<th>Key responsibilities</th>
</tr>
</thead>
</table>
| Chief Executive                            | - Has overall responsibility for Security within the CCG.  
- Ensures that adequate resources are available to implement the security strategy and policy.                                                                                                                     |
| Chief Finance Officer and Deputy Chief Officer | - As the voting member of the Governing Body is responsible for Security Management.  
- Is the nominated Officer lead for security at Board level.  
- Is the first point of contact with the Counter Fraud and Security Management Service (CFSMS).                                                                                                                             |
| Director of Governance & Compliance        | - Is the Senior Information Responsible Office (SIRO) and has responsibility for promoting security management work and awareness.  
- Authors, develops and presents to the relevant committees with board delegated responsibility any policy, strategy, procedure or development related to security issues.  
- Reviews and amends the security policy to ensure compliance with current guidance.  
- Initiates regular campaigns to highlight the importance of security and the responsibilities of all CCG staff.                                                                                                             |
| Directors                                  | - Ensure that security risk assessments are carried out within their areas and ensure that staff for whom they are responsible are aware of these risks  
- Implement preventative measures and appropriate action for persons who are suspected of committing a criminal offence, misconduct or other breach of security in contravention of the policies of the CCG.  
- Ensure staff awareness of their responsibilities under this policy.  
- Ensure staffs attend relevant training, which is a requirement of the Secretary of State’s directions.  
- Ensure that security arrangements within their Team are being observed and that deficiencies are reported through the CCG incident reporting system.  
- Actively review the security arrangements within their Team by carrying out routine audits themselves with the co-operation of staff organisations, in line with CCG risk assessment procedures.  
- Ensure that every member of staff obtains a security ID Badge and that the badge is worn and visible at all times whilst the staff member is on CCG premises.  
- Implement the recommendations from investigations, risk assessments and security alerts.                                                                                                                                 |
| Estates and Facilities Manager              | - Is the Security Liaison Officer for the CCG  
- Ensures adequate consultation regarding security arrangements are taken into account when converting or refurbishing existing builds.                                                                                                                |
<table>
<thead>
<tr>
<th><strong>Local Security Management Specialist (LSMS)</strong></th>
<th><strong>Deputy Director Governance &amp; Compliance</strong></th>
<th><strong>All staff</strong></th>
</tr>
</thead>
</table>
|  - Implement the recommendations from investigations, risk assessments and security alerts where required.  
  - Ensures there are appropriate systems in place to implement and review the CCG’s security policies and procedures  
  - Collaborate closely with the Deputy Director of Governance and Compliance on all security and emergency planning issues that are by their nature inter-connected and have the potential to impact on each other’s functions. |  - Reports directly to the Security Management Director and is responsible for liaising between the CCG and NHS Protect  
  - Is required to report to NHS Protect any weaknesses in security related systems of the NHS body or other matters which the LSMS considers may have implications for security management in the NHS.  
  - Provides competent advice on the CCG’s management of security.  
  - Reviews security policies.  
  - Conducts security risk assessments.  
  - Reviews security incidents and report all incidents of violence and aggression to NHS Protect (RAPS)  
  - the relevant committees  
  - Monitors progress made against recommendations arising from security audits |  - Responsible for familiarising themselves with any special security requirements relating to their place of work.  
  - Safeguard themselves, colleagues, visitors, clients etc., so far as is reasonably practicable.  
  - Ensure that neither equipment nor properties are put in jeopardy by their actions, either by instruction, example or behaviour.  
  - Co-operating in the completion of risk assessments.  
  - Comply with policies/procedures, control measures and safe systems of work.  
  - Comply with the principles and requirements of the Security Risk Management Process  
  - Report any security concerns/breaches or incidents as soon as possible  
  - Attend appropriate training sessions  
  - Provide support and co-operation with any investigations  
  - use all security equipment in accordance with any training and instructions given e.g. panic alarms  
  - Remain alert to the presence of unusual and |
unexplained packages, which cannot readily be identified. Any such package should be reported immediately to a supervisor or line manager. Under no circumstances should a suspect package be handled.

- Wear CCG identity badges at all times unless otherwise directed due to control of infection or personal safety.

Central to this policy is the responsibility that rests with the CCG Governing Body to ensure that the organisation has in place appropriate and reasonable measures to mitigate the security and crime risks that arise. As this policy will outline, clear responsibilities rest with all members of staff to ensure that they play their part in making the CCG a safe and secure environment for the delivery of the highest standard of patient care.

This policy applies to all full time and part time employees of the CCG, its partners, contractors or sub-contractors who provide services to the CCG (including temporary staff, clinical and non-clinical), students/trainees, volunteers, clinical attachments, apprentices, seconded staff and all other staff on placement within the CCG.

Furthermore, it incorporates patients (inpatients and outpatients), their relatives and visitors, including courier and delivery personnel.

In accordance with the requirements of the Health and Safety at Work Act, etc 1974 and the Management of Health and Safety at Work Regulations 1999, employers have a duty to ensure the health, safety, and welfare of their staff. The scope of this policy will not only apply to the specific requirements of NHS Protect but also to the statutory requirements of health and safety legislation. Therefore, this policy both enshrines and underpins the CCG's existing legal duties to protect staff and assets, as far as reasonably practicable, from the effects of criminal and security related incidents.

NHS Protect supports the NHS in ensuring that finite resources are used effectively in delivering good quality health care. In order to do this:

NHS Protect co-ordinates work to prevent crime in the NHS effectively and efficiently. This will include managing information and intelligence in all parts of the NHS and sharing it with relevant bodies so that, wherever possible, crime is prevented.

NHS Protect introduces measures to ensure there is a greater local accountability in preventing crime and that the benefit of localised investment is maximised in order to tackle crime. Greater local accountability will enable NHS Protect to co-ordinate and manage work to tackle crime against the NHS nationally, and to deal with complex crime through the National Investigation Service. The basis for this local accountability will be in legislation and commissioning contracts, which will set out the responsibilities of commissioners and providers respectively.
6.0 Procedure

6.1 G&W CCG Security Priority

Six specific areas of action have been identified as a priority to address in compliance with NHS Protect priorities:

- Tackling violence and aggression against staff
- Protecting NHS property and assets
- Securing drugs, prescription forms and hazardous materials
- Unauthorised access to premises & assets
- Lone Working
- Verbal Abuse
- Office Environment

6.2 Risk Management

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

Risk assessment:

- Reviews the various activities of the CCG and identifies critical areas for the organisation
- Identifies the risks that exist
  a. What could go wrong?
  b. How could it happen?
  c. What would be the effect?
- Assesses those risks for potential frequency and severity.
- Eliminates the risks that can be eliminated.
- Identifies how remaining risks can be mitigated or managed
- Develops and delivers a plan for implementing the identified changes.
- Provides current measurement and assists target setting for reduction in risks.

The CCG will carry out appropriate risk scoping on physical security of premises and assets every year. Following a risk assessment on premises or assets an action plan will be developed with timescales and nominated persons to carry out agreed action. The plan is kept by the Estates/Facilities/Corporate manager.

- If new premises or assets are commissioned within the CCG these will be risk assessed prior to operational use of them, in line with this policy.
- Help and support with undertaking a security risk assessment is available from the LSMS. Managers can also receive risk assessment training.

Copies of risk assessments and the action plan are sent to the LSMS for collation and review.
6.3 Incident Reporting

All security incidents and near-misses must be reported on the CCG’s incident reporting system, through a manual form, following the CCG’s Incident Reporting and Management Policy. Reports to NHS Protect (RAPS) will be made by the LSMS.

All incidents are reviewed by the LSMS and the Risk Manager.

6.4 Access Controls

A Security Risk Management Assessment of access controls to CCG premises will be undertaken annually. The assessment will include:

- Physical Access
- Restricting Physical Access
- Security Equipment for Access Control
- Accessing Monitoring by Staff

6.5 Identification

The CCG currently has a protocol in regard that all staff must wear a name badge (see 6.14). There is a:

- Basic System for identification purposes only
- Advance System for identification and access control
- Pass system for authorised visitors and contractors.

6.6 Training

Directors are responsible for ensuring all their staff receive the type of initial and refresher training that is commensurate with their role(s). Staff must keep a record of all training in their portfolio. Relevant aspects of this policy will also be covered in the Corporate Induction.

Staff with responsibility for security, have access to specialist guidance in implementing security and crime prevention strategies.

6.7 Security Measures

6.7.1. Conflict Resolution

The CCG has policies for Violence and Aggression, bullying and harassment at work.

6.7.2. Keys & Digital Lock codes

The following principles provide adequate control over keys and digital Lock code numbers with safety, and ensure accountability:

- The digital lock keypad access code to the CCG main entrance doors will be provided to the on-call Managers and authorised staff only. The code should not be divulged to anyone unless approved by a Director
- Other keys should remain under the control of the relevant department and should be accounted for in an orderly system.
• At the central key safe, where unused and duplicate keys are kept by the Estates & Facilities Manager, keys should be held in a lockable key case and a record maintained of the issue and return of keys.
• No extra keys should be cut to locks without the approval of the Estates & Facilities Manager.

6.7.3. **CCTV**
Closed circuit television systems are in operation throughout the CCG. Separate guidance has been produced which identifies the purpose, accountability, management and monitoring of the systems (CCTV Code of Practice).

6.7.4. **Property**
Property of Staff and visitors: If private property has been stolen, it is the owner’s and not the CCG’s responsibility to report the matter to the Police.

The CCG does not accept liability for the loss of, or damage to private property including motor vehicles or other modes of transport. The CCG will take all reasonable steps to safeguard vehicles but, motor vehicles and other modes of transport brought onto the CCG’s premises are done so entirely at the owner’s risk.

Staff are advised to take adequate precautions to ensure the safety of their possessions and not bring valuables to work. Where a lockable drawer/cupboard/locker has been provided for personal use, the individual to whom it is allocated is advised to use this.

Staff must report any loss or damage to their belongings and co-operate in any consequent enquiry into the loss or damage.

CCG Property: It is an offence for members of staff to remove property belonging to the CCG without written authority. Failure to seek authority from line management could result in disciplinary action or criminal proceedings being taken. Staff must take all reasonable steps to safeguard CCG property whilst in their care. If theft or malicious damage to NHS property is suspected to have been committed, the Police will be informed.

6.7.5. **Inventories and Security Marking of Valuable Equipment**
Inventories of all equipment considered to be of sufficient value or operational necessity are maintained. Valuable and/or attractive items of equipment should be marked by the CCG to deter theft and assist in identification in the event of loss or theft. The LSMS can advise on suitable marking equipment.

6.7.6. **Computer Security**
This is included in the Information Security Policy.

6.7.7. **Fraud**
Fraud is a serious offence and diverts NHS funds away from patient care. All allegations of fraud are taken seriously by the CCG and offenders face both disciplinary action and prosecution.
The CCG Standing Financial Instructions must be followed at all times. Staff suspecting fraud should contact the Counter Fraud Specialist to discuss their concerns.
6.7.8. Purchase of Security Systems
Divisions/Departments must consult the LSMS and the Estates/Facilities Manager before purchasing security equipment or systems (such as automated access control systems, including video/intercom systems and swipe card readers; CCTV, security lighting, and intruder alarms). This is to ensure compatibility of the system with existing systems and compliance with other statutory regulations and guidance.

6.8 Monitoring
The LSMS reviews all risk assessments and all incidents relating to security of premises and assets and reports to relevant staff and committees:

- Risk assessments
  - Trends
  - Progress with action plans
  - Blocks to implementation

- Incidents
  - Number
  - Trends
  - Progress with action plans
  - Blocks to implementation.

The relevant committee will ensure implementation plans are completed.

6.9. Sanctions and Recovery
The CCG will pursue sanctions and a recovery of losses occurred through crime where possible, in order to re-invest in patient care. This could involve different paths including disciplinary action, criminal convictions, injunctions, etc. Where needed, the CCG will work together with other relevant parties, such as the police, CPS and NHS Protect, to ensure a positive outcome.

6.10 Premises and Asset Security Guidelines
The security of all CCG premises is the responsibility of all staff and a general level of awareness and compliance with the security policy and any specific security measures is essential. Any concerns or untoward findings should be reported immediately to the Estates/Facilities Manager responsible for the site and/or service.

6.11. Building Security
All staff should ensure that when a security concern arises the CCG’s incident reporting policy should be followed at the earliest opportunity. This will ensure that the relevant staff are informed of security incidents and appropriate action can be taken. This includes addressing the raised concerns and instigating any necessary action in accordance with the provisions of this policy and his/her responsibilities. If they are confronted with a situation that is out of their control, they should remove themselves to a place of safety and contact the Police.
All members of staff should ensure that their work areas are secured at the end of the working day (where applicable) and that departmental keys are held in a secure place at all times.

The loss of any key(s) or security identification badges must be reported to the appropriate manager and to the CCG’s Security Service as soon as the loss is discovered. It is important to avoid delay so as to mitigate the security risks that may arise from these losses.

Members of staff, who require specific access through any door, which is controlled via digital door locks or access control systems, will be issued with the appropriate code numbers or have their Security Identification cards reconfigured to facilitate access. Under no circumstances must Digital Code numbers and/or Security Identification badges be issued to unauthorised personnel.

It will be the responsibility of the relevant manager to ensure that all access codes are changed:

- a minimum of every 6 months, or
- whenever the code has or is suspected to have become compromised, or
- following the dismissal and/or suspension of a member of staff.

The control of keys and their replacements in other areas is the responsibility of the local manager and the Estates and Facilities Manager.

The CCG has provided access control systems across the sites to facilitate electronic security for nominated internal and external doors. In practice this means that some doors are normally held closed and locked electro-magnetically. CCG security badges are computer-coded and act as a proximity device to open these doors for a short period. All the doors are fitted with door-closers. The system is monitored to prevent abuse.

The access control systems are managed by the Estates and Facilities Manager. The level of access provided to staff will be agreed between the Estates and Facilities Manager and the local manager. It is a duty of the Departmental Manager to ensure that both the Estates/Facilities Manager and HR are notified of a member of staff either leaving or subject of suspension in order that the relevant staff can cancel all access levels for that member of staff and that the cancellation becomes effective from the end of their last working day. The manager should also take possession of the staff members ID card.

It is CCG policy to monitor all access points/entrances to the premises by the use of CCTV and to establish clearly signposted exits for emergencies. CCTV and signage are subject to continual review.

Members of staff should be aware of anyone trying to ‘tailgate’ – i.e. gain access to a controlled access area by closely following them as they enter. If the person is not wearing a CCG ID badge or is not a confirmed authorised visitor, he/she should be asked to:
- Wait at the door or in a designated waiting area
- Give details of the person, with whom they have an appointment
- Await the arrival of an identified member of staff to escort him / her into the controlled access area
- At the end of the appointment / meeting, the visitor should be escorted out of the controlled access area.
- Should any concerns arise the LSMS should be informed.


All staff should familiarise themselves with the Building Access Protocol policy which is available on the CCG website. The policy explains in detail the process for gaining access to the office and the daily unlocking and locking procedures for Dominion House.

6.13. Car park Security

The car park in Dominion House is a common area and is managed/maintained by the Landlord’s Managing Agents (CBREMS). CCG subscribe to the principles of secure car parking initiatives and guidelines for staff:

- Spaces are allocated to specific members of staff.
- Entry to the car park is access controlled by the Landlord’s access reader system.
- The safety and security of the car park is subject to continual review.
- Report any concerns to your Estate and Facilities Manager.
- Avoid leaving valuable items in your vehicle or store.


CCG staff Identification cards must be worn openly at all times. Identification cards will be issued to all new starters on their first day within the CCG, during their induction. It is the responsibility of the recruiting Manager, to complete all relevant documentation and to confirm ID card requirements prior to appointment start date.

All losses must be reported immediately by email to the Estates and Facilities or IG Manager. Any changes in access requirements for any member of staff must be requested by email from by their line Manager to the Estate/Facilities Manager.

6.15. Visitors and Contract staff

6.15.1. Visitors

All Visitors must call at the Reception on the 3rd floor, where they will be greeted by a member of the Admin team (during working hours) who will arrange for the department or relevant staff member to be contacted and informed of the arrival of the visitor(s). Visitor(s) will be required to sign in, in a log in book.

The visitor(s) should wait in the reception area until they are escorted to their destination by a member of staff of the department they are visiting. At the end of the visit/meeting, the visitor(s) will be escorted back to the reception area, where the visitor is requested to sign out.
6.15.2. Couriers and goods delivery
The effective supervision of couriers and the delivery of goods to CCG premises is fundamental to the CCG Security objectives. It is the duty of all staff to ensure strict compliance with the provisions of this section of the policy.

Couriers are not permitted access to any area subject of access control unless escorted by a member of the department, subject of the courier service. Furthermore couriers are not permitted to remain unsupervised in any office or access controlled area where the integrity of the CCG assets, personal or other confidential information including patient information of a commercial value is potentially at risk.

6.16. Asset security

6.16.1. Delivery of Goods
It is the duty of the manager responsible for the department ordering such goods to ensure:

- Agreed location for delivery and where practicable date and time of delivery
- Goods checked against delivery sheets prior to signature of receipt for accuracy
- That only the goods, subject of that delivery order are signed for
- That the goods signed for are in good order
- Safe storage of the goods until they are delivered to the specific department. The safe and secure delivery of goods to all CCG premises is fundamental to the delivery of the services the CCG provides.

6.16.2. CCG Assets
The CCG will maintain asset registers and will ensure the security of its assets, as per Standing Financial and Local Instructions. It is the responsibility of the managers of specific services or departments to have an updated asset tracking register detailing the location and or person have custody of any given asset at any specific time. Every employee has a responsibility for the security of the CCG property they use.

Any damage to the CCG’s premises and equipment, or any loss of equipment, stores or supplies must be reported immediately to the manager responsible for the service. This includes notification to the LSMS and the Police as necessary.

Where practicable, assets should be suitably marked as CCG property (refer to Standing Financial Instructions).

It is the responsibility of Directors to ensure that CCG assets such as lap tops, mobile phones and any other devices are surrendered prior to a member of staff leaving the organisation or after the period of need has expired.

On those occasions where assets are removed from CCG premises the person in whose possession the asset is found must have a written authority from the senior/line manager to remove such an asset from CCG premises or the normal place of work.
6.16.3. Staff Property
Each member of staff is responsible for the safe keeping of his / her own property. Staff should consider what personal belongings they need to bring to work and ensure they are held securely in the building. The loss/theft of personal belongings must be reported immediately to the employee’s line manager, the LSMS informed and an incident report completed. Where appropriate, the Police should be contacted. Desk pedestals and or lockers will be provided to all staff.

6.16.4 Lost and found property
In the event that property becomes lost or handed in, staff should contact the Estates and Facilities Manager who will hold the property in a secure place and endeavour to contact the owner by emailing all staff.

7. CCTV Policy

7.1. Introduction
This document sets out the appropriate actions and procedures, which must be followed to comply with the Data Protection Act in respect of the use of CCTV (closed circuit television) camera surveillance in the CCG.

The Data Protection Act 1998 came into force on the 1st March 2000 and contains broader definitions than those of its predecessor (1984) Act and more readily covers the processing of images of individuals caught by CCTV cameras. The changes in data protection legislation mean that legally enforceable standards will apply to the collection and processing of images relating to individuals.

If CCTV shows a recognisable person then it is generally classed as Personal Data and is covered by the Data Protection Act. Anyone who believes they have been filmed by CCTV is entitled to ask for a copy of the images, subject to the exemptions on access under the act. They do not have the right of instant access, and must abide by the appropriate data protection procedures. In some cases a permanent copy of the information containing the images of the data subject need not be provided if a viewing of the footage has been agreed instead.

An important new feature of the legislation is the production of a CCTV Code of Practice by the Office of the Information Commissioner. This Code of Practice sets out the measures which must be adopted to comply with the Data Protection Act 1998. This goes on to give guidance for the following of good data protection practice. The Code of Practice has the dual purpose of assisting operators of CCTV systems to understand their legal obligations while also reassuring the public about the safeguards that should be in place.
7.2. Purpose, Aims and objectives

The purpose of this policy is to ensure:

- That any CCTV system is not abused or misused.
- That CCTV is correctly and appropriately installed and operated.

The overall aim of CCTV schemes is to help in the reduction of, and investigation of crime, to protect CCG staff and to protect CCG premises from criminal activities. The purposes are in accordance with the following rationale:

- To assist in the prevention and detection of crime against both persons and property.
- To facilitate the identification, apprehension and prosecution of offenders in relation to crime.
- To ensure the security of property belonging to the CCG and to employees and visitors of the CCG.

This policy covers all staff within the CCG and others working on behalf of the organisation, in respect of the use of CCTV Camera surveillance.

The objective of the policy is to ensure the use of CCTV cameras throughout the CCG will be in installed and used in compliance with the principles of the Data Protection Act 1998, Human Rights Act 1998, Regulation and Investigatory Powers Act 2000 and other relevant legislation.

The Regulation of Investigatory Powers Act 2000 regulates the use of covert/directed surveillance and is subject to a strict code of practice. Use of CCTV in these circumstances or for any other reason other than that authorised in accordance with this policy is not covered by this policy and in such circumstances further guidance should be sought.

7.3. Purpose of the system

The purpose of the CCG’s CCTV scheme(s) as notified under the Data Protection Act include:

- Support Police in a bid to prevent or detect crime or disorder;
- Assist in the identification, apprehension and prosecution of offenders (including use of images as evidence in criminal proceedings);
- Increase personal staff/public safety and reduce fear of crime;
- Protect the premises and their assets;

Prior to considering compliance with the principles of the Data Protection Act, a user of CCTV or similar surveillance equipment, will need to determine two criteria:

- The type of personal data being processed i.e. is there any personal data which falls within the definition of sensitive personal data as defined by Section 2 of the Act;
‘Sensitive personal data’ in relation to this policy is images stored either digitally or on video tape.

Under the data Protection Act principles, the personal data is being processed (including CCTV images) must be:

- fairly and lawfully processed;
- processed for limited purposes and not in any manner incompatible with those purposes;
- adequate, relevant and not excessive;
- accurate;
- not kept for longer than is necessary
- processed in accordance with individual’s rights;
- secure;
- not transferred to countries without adequate protection;

The Data Protection Officer (Head of Information Governance) will ensure that CCTV Systems are registered with the Information Commissioner under the terms of the Data Protection Act 1998 and will comply with the requirements the Data Protection Act.

All schemes will operate in accordance with the guidelines set out in the “CCTV Code of Practice” published by the Office of the Information Commissioner, a copy of which is available from the Data Protection Officer or direct from the Information Commissioner’s website:

http://ico.org.uk/for_organisations/data_protection/topic_guides/cctv

The CCG must adhere to the following guidelines, to conform to this Code of Practice:

- Managers operating such schemes will be responsible for overseeing that monitoring of all images are done so in accordance with this policy and that suitable operation, backup, retention, destruction and maintenance of all storage media is conducted in accordance with written operational procedure.
- Cameras will not be hidden from view and appropriate steps must be taken to inform the public of the presence of the system and its ownership at all times.
- To ensure cameras will operate so that they only capture images relevant to the purpose for which that particular scheme has been established and approved.
- Images from the cameras are appropriately recorded in accordance with existing operational procedures.
- There is no sound recording undertaken from any part of the system.

7.4. Roles and Responsibilities

<table>
<thead>
<tr>
<th>Party</th>
<th>Key responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Governing Body</td>
<td>• The implementation of policy, monitoring its effectiveness and ensuring the CCTV policy is</td>
</tr>
<tr>
<td>Role</td>
<td>Responsibilities</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Available to staff and the general public for reference purposes.  
Discharging this responsibility through the Chief Finance Officer | Chief Executive  
Legal responsibility for the CCTV schemes. However the Data Protection Officer has responsibility for the day to day compliance with the requirements of the CCTV Code of Practice. |
| Responding to complaints relating to processing under the Data Protection Act.  
Responding to Subject Access requests in accordance with Data Protection legislation. | Head of Information Governance |
| Ensuring that the policy and Code of Practice are adhered to and monitored. | Deputy Director of Governance and Compliance |
| Overseeing that monitoring of all images are done so in accordance with this policy and that suitable operation, backup, retention, destruction and maintenance of all storage media is conducted in accordance with written operational procedure.  
Registering with the Information Governance Coordinator any new or modifications to CCTV Systems or related information required for registering.  
Following this policy and producing local protocols for the use of CCTV Systems within their area of control.  
Responding to Subject Access requests from the IG Manager in accordance with Trust policy. | Estates and Facilities Manager |
| Review CCTV systems in place and advise on whether they are fit for purpose | Local Security Management Specialist |

### 7.5. CCTV system

#### 7.5.1. Initial Assessment Procedures

The purposes of the CCG’s CCTV scheme(s) as notified under the Data Protection Act include:

- Support Police in a bid to prevent or detect crime or disorder;
- Assist in the identification, apprehension and prosecution of offenders (including use of images as evidence in criminal proceedings);
- To increase personal staff/patient/public safety and reduce fear of crime;
- Protect the premises and their assets;

Prior to any camera installation the Data Protection Co-ordinator will ensure that the installation complies with the Data Protection Act and CCTV Code of Practice.

#### 7.5.2. Type of CCTV System
The CCG operates a DVR/networked CCTV system. The DVR/server is kept in a restricted area.

7.5.3. **Operation of the Systems**

The data controller will be the CCG. CCTV cameras within the CCG will not be used for covert surveillance unless authorised, any requests to do so must be made through the Head of Information Governance. All covert surveillance undertaken by NHS bodies must have appropriate authorisation. Obtaining authorisation ensures that the operation is carried out in accordance with the law and is subject to stringent safeguards against abuse. It will also make the action less vulnerable to challenges under the Human Rights Act 1998.

7.5.4. **Siting the Cameras**

It is essential that the location of the equipment is carefully considered, because the way in which images are captured will need to comply with the Data Protection Act. All cameras are located in prominent positions within public and staff view.

Training programmes are facilitated for the staff on the Data Protection Act and CCTV Code of practice.

Signage has been placed on all entrance points to the premises to ensure staff and visitors are aware they are entering an area that is covered by CCTV surveillance equipment. The signage must include details on the purpose, organisation and contact details.

7.5.5 **Quality of the Images**

It is important that the images produced by the equipment are as clear as possible in order that they are effective for the purpose(s) for which they are intended. This is why it is essential that the purpose of the scheme is clearly identified. For example if a system has been installed to prevent and detect crime, then it is essential that the images are adequate for that purpose.

It is recommended that only companies approved by organisations such as the National Security Inspectorate (NSI) and the Security Systems and Alarms Inspectorate Board (SSAIB) are used to supply and install CCTV systems. Upon installation all equipment is tested to ensure that only the designated areas are monitored and high quality pictures are available in live and play back mode. Cameras should be properly maintained and serviced to ensure that clear images are recorded. A record of such maintenance should be retained.

All faulty equipment within the CCTV system that could affect picture or recording quality should be repaired or replaced as soon as practically possible. Failure to do so not only compromises the efficiency of the system, but also breaches two of the principles of the Data Protection Act 1998 – that data should be adequate and accurate.

If a time/date facility is used on the system regular reviews must take place to make sure that the system is displaying the correct time and date.
7.5.6. Retention and processing of the images
Images, which are not required for the purpose(s) for which the equipment is being used, should not be retained for longer than is necessary, but generally 30 days, after which they are automatically overwritten. While images are retained, it is essential that their integrity be maintained, whether it is to ensure their evidential value or to protect the rights of people whose images may have been recorded. It is therefore important that access to and security of the images is controlled in accordance with the requirements of the 1998 Act.

Where the images are required for evidential purposes in legal or disciplinary proceedings they will be properly processed following consultation with the Data Protection Officer. The recording medium is for digital images copied to disc or memory stick, placed in a sealed envelope signed and dated and stored securely until completion of the investigation. Viewing of images is controlled by the Head of Information Governance.

Tapes or images will not be made available to the media, for commercial gain or entertainment.

7.6. Access to images
Images are covered in the CCG’s Subject Access Request policy.

7.7. Documentation
Copies of all documentation and records relating to the CCTV scheme will initially be dealt with by the Head of Information Governance.

Where these cannot be resolved the individual has the right to write to the office of the Information Commissioner.

7.8 Standard Operating Procedures CCTV
- Cameras must always be operated so that they will only capture the images relevant to the purpose for which the particular scheme has been established and approved.
- Cameras and recording equipment should be properly maintained in accordance with manufacturers’ guidance to ensure that clear images are recorded.
- Cameras should be protected from vandalism in order to ensure that they remain in good working order.
- If a camera/equipment is damaged or faulty there should be a separate local procedure for:
  - Defining the individual (s) responsible for ensuring the camera/equipment is fixed.
  - Ensuring the camera/equipment is fixed within a specific time period.
  - Monitoring and overseeing the quality of the maintenance work.
- Cameras must be located in prominent locations in order that the cameras only monitor those areas for which they were intended. Cameras should not have sight of any private premises without the express written permission of the owner of those premises, unless they come into view as part of a wide-angle or long shot only. If cameras can be adjusted by the operator(s), consideration should be
given to restricting their movement so that they cannot be manipulated to overlook areas that are not intended to be monitored.

- When selecting external camera positions, care should be taken to ensure that foliage does not create blind spots at certain times of the year, a good position in winter may not be a good position in spring and summer.

**7.8.1 Operators**

- All operators of CCTV equipment should be trained in their responsibilities in accordance with the CCG policy and this procedure.
- All staff involved in the handling of the CCTV equipment, both directly employed and contracted, will be made aware of the sensitivity of handling CCTV images and recordings.

**7.8.2 Training**

- Guidance in the requirements of the law on Data Protection will be given to staff who are required to manage and work the CCTV systems.
- Staff will be fully briefed and trained in respect of all functions, both operational and administrative relating to CCTV control operation.
- Training by camera installers will also be provided as appropriate.

**7.8.3 Maintenance**

- A comprehensive maintenance log will be kept which records all adjustments/alterations/non-availability of CCTV cameras.
- If the system records location/time/date, these will be periodically checked for accuracy and adjusted accordingly. In the case of alterations due to “British Summer Time” the system should, as a matter of course, be checked for accuracy.
- A review must be undertaken at least annually against the stated purpose of the identified scheme.

**7.8.4 Access**

- All staff should be made aware of the procedures for granting access requests to recorded images or the viewing capabilities of CCTV schemes (as per CCTV Policy). All such requests (in the first instance) should be notified promptly to the Data Protection Officer in writing.
- Criteria for the viewing of images by non-security related personnel:
  At the discretion of the responsible officer, individuals may be allowed to view images:
  
  - If they are investigating an untoward incident
  - To identify persons relating to an incident

  Areas which would normally result in permission being refused include:
  
  - Where the person wishing to view has no connection with the incident or has no management role relating to an incident.
  - Where viewing is purely salacious
  - Where the performance of a member of staff not relating to crime, fraud or the investigation of untoward incidents is involved.
8.0 Procedure for dealing with bomb threats, suspect packages and other threats

8.1. Introduction

NHS organisations including hospitals and other premises have long regarded themselves as immune to bomb threats and other gross acts of violence.

However while bomb threats and such acts are fortunately considered rare, the risk remains and therefore an effective bomb threat strategy is required to ensure the following:

- That the CCG is vigilant to situations where a threat may be increased.
- That all staff are made aware of the actions to be taken if a bomb threat is received.
- That an effective evacuation procedure and recovery plan is identified in cases of actual bombs being found.

The threat of incendiary and explosive devices may arise from acts of terrorism connected with international issues. There is a serious and sustained threat from international terrorism to the UK and UK interests overseas.

As well as the international and domestic terrorist groups, the risk or threat can be posed by individuals who may target the CCG for any number of reasons including revenge, blackmail, and dissatisfaction or for reasons of mental illness.

Whilst few, if any, devices have been found in NHS premises to date, NHS organisations are clearly a potential target for terrorists who want to gain publicity for their cause.

Given the disruption and anxiety the threat of a bomb could cause, it is essential that the CCG is prepared as much as it can be for such an event occurring.

This procedure may need to be used in conjunction with the CCG’s Incident Management Plan and Lockdown Procedure.

The Deputy Director of Governance and Compliance and the Estates and Facilities Manager receive alerts in the event UK threat level changes and will review arrangements should this occur.

8.2. Purpose, aims and objectives

This procedure has been developed to ensure that sufficient information is obtained wherever possible to determine whether the threat is a credible one or a malicious hoax and also that staff know how to respond.
The purpose of this procedure is:

- To reinforce the CCG’s commitment to doing all that it reasonably can to safeguard its staff and assets.
- To provide basic guidance for controlling and dealing with situations involving any bomb threats that may be received.
- To provide basic guidance for controlling and dealing with situations involving any suspicious packages that may be received or discovered.
- To promote an understanding amongst all grades of staff of bomb threats and outline the action to be taken in the event of a bomb alert.
- To promote an understanding amongst all grades of staff of what constitutes a suspicious package and the action to be taken following the receipt or discovery of suspicious packages.
- To identify the responsibilities of key staff within these procedures.
- To ensure that such incidents are investigated fully in line with the Incident Reporting Procedure.

### 8.3. Roles and Responsibilities

<table>
<thead>
<tr>
<th>Party</th>
<th>Key responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chief Executive</td>
<td>Overall responsibility for the safety of CCG premises, visitors and staff. He/she has delegated the executive lead for security and Business Continuity planning to the SMD.</td>
</tr>
<tr>
<td>Chief Finance Officer</td>
<td>Overall responsibility for managing an incident involving either a bomb threat or suspect package and ensuring continuation of services as far as possible. He/She will take responsibility for ensuring preparations are made to respond to an incident of this type.</td>
</tr>
</tbody>
</table>
| All staff              | Responsible for observing the Procedure for Dealing with Bomb Threats, Suspect Packages, and other Threats at all times. It is imperative that all staff understand what to do in the event of this kind of threat to ensure the safety of their colleagues, the general public and themselves. It is the responsibility of all staff to:  
  - Always keep areas that are restricted from unauthorised persons locked. This includes cupboards, medicines etc.  
  - As far as is practical keep items where packages could be hidden, away from such threats this includes boxes, delivery trolleys etc.  
  - Keep areas where security is a risk well lit, especially at night.  
  - Rubbish must not be allowed to accumulate in any area.  
  - Report to their line manager if they observe any suspicious activity.  
  - Make themselves aware of the surroundings in which they work.  
  - Draw attention to incidents relating to suspicious devices etc. |
Any person acting suspiciously should be challenged if safe to do so and/or reported to the Police
- Any suspicious packages that cannot be identified must be reported to the Estates/Facilities manager, Risk manager or the Police
- Any member of staff who receives a bomb threat must report it immediately to the Police via 999

### 8.4. General Guidelines

- If a suspicious object is found - **DO NOT TOUCH IT!!**
- Unless there is an IMMEDIATE THREAT (such as fire) - do not evacuate areas unless told to do so by security staff or the police.
- Dependent on the level of threat received staff may be asked to assist in searching areas and assist the emergency services to locate any suspicious items. Any such assistance will be asked for on a voluntary basis.

### 8.5. The Threat

Bomb threats usually originate as the result of:

- a telephone call or letter which may be anonymous, alleging that a bomb has been placed in a particular location.
- the discovery of an item suspected of being or containing a bomb and for which no warning has been received, this includes letter bombs and car bombs.

Planning is based on receipt of the threat, its evaluation and action to deal with the incident.

Each telephone threat call, written message or other means of communication alleging that a bomb has been or will be placed must be considered credible and serious, it should be investigated immediately and the police informed.

### 8.6. Actions to be taken by person receiving the call

Telephone calls notifying a bomb threat may be received from the Police, newspapers or other legitimate sources. These sources will normally ask to be connected to a Senior Manager and should be referred to the Senior Manager/person in charge of the area.

Any person who receives a bomb threat should:

- Stay calm and listen to what is said.
- Record the details as soon as practically possible.
- Attempt to keep the caller on the line as long as possible and attempt to obtain as much information as possible.
- Ensure that the exact words are recorded including any code words given by the caller even if they mean nothing to the person receiving the call at the time.
The caller may ring off immediately after giving the message but whoever takes the call should nevertheless try to get a response to the following questions and write down the answer:

- Where is the bomb?
- What time will it go off?
- What does it look like?
- Why are you doing it?

After the call has been completed, fill in any further details on the form and then follow the procedures as detailed below. All paperwork relating to the incident must be retained no matter how insignificant it might seem, post-it notes, rough drafts etc. These need to be attached to the Aide Memoir and given to the Director handling the incident.

8.7. Reporting the incident

In all cases, whether or not you consider the threat to be credible, you should contact:

- The Police immediately (giving details entered on the form) via 999.
- The Fire Brigade.
- The relevant Directors, as indicated in the Incident Reporting Policy. The On-Call Manager will assume responsibility for managing the incident and will decide if the Major Incident cascade needs to be invoked and/or whether to evacuate premises.
- The Estates and Facilities Manager (both NHS Property Services and CCG staff).
- Communications Manager.
- The relevant staff as detailed in the Incident Reporting Policy should also be notified.

8.8. Threats received by other means

Bomb threats may be received by means other than telephone. In cases where it is in the form of a hand written or typed note, the document and all material received with it should be carefully preserved for fingerprint examination. Unnecessary handling or other careless acts will only destroy evidence and make the task of tracing the originator more difficult if not impossible. The note/letter should be placed in a plastic bag and sealed.

The person receiving a bomb threat directly or who overhears one made should:

- Notify their manager/supervisor immediately
- Keep the person making the threat or indicating knowledge of such a threat under surveillance (if possible, without putting themselves at any risk) until police attends
- Note the age, height, weight, sex, colouring of eyes, skin and hair, clothing and any unusual characteristics such as lameness, twitching or peculiarities of the person under surveillance.
- If the person making the threat leaves the scene, note the transportation used private car, taxi etc. Note the make, model, colour and registration number. If a
bus or taxi is used, note the name of the company and any numbers on the vehicle.

Very often, terrorists issue telephone warnings to organisations, which would not themselves, be affected by the explosion, they are warning about. In these circumstances the response is just as important because the safety of others may depend upon it.

8.9. Discovery of Suspect Packages

Where no warning has been received but a suspect package has been found, staff should inform the Police and the Chief Executive or his/her deputy. The procedure relating to the evacuation outlined above should be followed.

8.10. Car Bombs

The car bomb is potentially a very lethal weapon and if a threat is confirmed by the Police, it will be necessary to control and search every vehicle entering the premises concerned. Drivers who refuse to co-operate may be refused entry. The police and security manager will have consultations with senior management to decide on appropriate counter measures.

All vehicles are capable of carrying a large bomb. For this reason, any vehicle that is parked outside a recognised car parking area, next to a building should be treated with suspicion.

8.11. Return area to all Clear/Stand down

After the time of the threatened explosion has passed and the search (if made) has been completed, the person in charge on the advice from the Police should declare a stand down.

The person in charge should ensure that all concerned, in particular the Ambulance, Fire and Police services are advised as soon as possible after the stand down is declared. Staff can only return to the area when the all clear has been given by the person in charge of managing the incident (in consultation with the Police Duty Officer).

8.12. Debrief

A full debrief will be set up by the CCG Local Security Management Specialist (LSMS) TIAA after any bomb threat or incident and the Bomb Threat Procedure should be updated as necessary.

8.13. Bomb Threat and the Law

The vast majority of bomb threats are hoaxes. Making such malicious calls is an offence contrary to Section 51 of the Criminal Law Act 1977 and should always be reported to the police.

8.14.1. General Advice on Mail
Sensible precautions should always be used in inspecting and opening mail or packages. IF YOU ARE IN DOUBT ABOUT A PACKAGE DO NOT TOUCH IT, MOVE IT OR OPEN IT, CALL THE POLICE ON 999.

Official UK Government guidance about opening mail delivered by post or courier is as follows:

- Look out for suspicious envelopes or packages (see below for some triggers of suspicion)
- Open all mail with a letter opener or other method that is least likely to disturb contents.
- Open letters and packages with a minimum amount of movement
- Do not blow into envelopes or shake or pour out contents.
- Keep hands away from nose and mouth while opening mail.
- Wash hands after handling mail.

8.14.2. What types of letters and packages may be suspect:
- Any envelopes or packages with suspicious or threatening messages written on it.
- Grease marks on the envelope or wrapping.
- Envelopes that are lopsided, rigid, bulky, discoloured, have an obvious strange odour or feel like they contain powder.
- An unusual odour, such as almonds or machine oil
- Unexpected envelopes from foreign countries.
- No postage stamp, no franking, no cancelling of the postage stamp.
- Improper spelling of common names, places or titles.
- The envelope or package is heavy for its size
- The package has been excessively wrapped
- There are too many stamps for the weight of the package.
- Hand written envelopes/packages from an unknown source particularly if addressed to an individual and marked personal or addressee only.

8.14.3. What to do if you discover Suspect Mail
Generally, because of what has already been violent handling through postal channels, there is no immediate danger from such a device once it is identified and isolated, providing nobody attempts to open it or cause further unnecessary handling or contamination by water, sand, chemicals or gaseous substances.

Immediate actions:

- DO NOT OPEN THE ENVELOPE OR PACKAGE
- NOTIFY your manager who will advise on further management – if he/she confirms the risk CALL THE POLICE ON 999 IMMEDIATELY.
- Do NOT take the letter / package to the police

8.14.4. Action in the event of opening a package/envelope which contains suspicious material, or finding an already opened package.
- Do not touch the package further or move it to another location
- CALL THE POLICE ON 999 IMMEDIATELY
• Shut windows and doors in the room and leave the room, but keep yourself separate from others and available for medical examination.
• Switch off any room air conditioning system.
• If there has been a suspected biological contamination, ensure that personnel outside the room are evacuated as soon as possible and ensure individuals in the contaminated room are evacuated to an adjacent unoccupied room away from the hazard.
• If there has been a suspected chemical incident ensure personnel leave the room as quickly as possible. Possible signs that people have been exposed will be streaming eyes, coughs and irritated skin. Seek immediate medical advice.
• Notify the On-call ESTATES PERSON who should:
  o Close all fire doors within the vicinity.
  o Close all windows within the vicinity.
In addition it is advised that:

• You should not clean up any spilled powder.
• If clothing is heavily contaminated, do not attempt to brush off any powder—it is better to remove the clothing carefully during decontamination.

8.15. Chemical / Biological Material.

What to do if anyone believes they have been exposed to

• Remain calm
• Do not touch eyes, nose or any other part of the body
• Wash your hands in ordinary soapy water where facilities are provided, but staff movement outside contained locations should be avoided as much as possible.
• Notify police immediately using the 999 system.
• Keep all persons exposed to the material separate from others and available for medical attention.
• Other people should assemble at a safe distance from the incident. They should not leave the area and should continue to be guided by the police and other emergency services.

8.16. Dealing with the Media

Reporting the incident must be factual and accurate. All media requests for information should be referred to the CCG’s Communication Manager who will ensure the best line of response to meet the any press enquiries.

8.17. Staff Training

All staff should be aware of this policy.

In addition, an action card should be displayed in the post room, summarising actions in case of a mail threat or a suspect package.

8.18. Post-Incident Review

It is important that, whenever an incident occurs as described in this Policy a post-incident review covering all aspects of action taken – from raising awareness
amongst staff about what to do through to establishing further deterrent and preventative measures.

9. **Lockdown Policy**

9.1. **Introduction**

Lockdown is the process in which the organisation temporarily adopts increased control and restrictions over access to and egress from its buildings. It can be used to prevent the escalation of certain types of incidents and to reduce the risk of danger to visitors and staff. To be effective a lockdown will need to be declared and implemented quickly and resourced by both CCG and police staff possibly for some time.

This policy and procedure may need to be used in conjunction with the CCG incident management plan.

The decision to lockdown the CCG or part of the CCG will be considered when extraordinary circumstances exist including:

- The need to contain or isolate a communicable disease or hazard within the CCG
- The presence of a Chemical, Biological, Radiological or Nuclear (CBRN) agent within the CCG which poses a threat to patient’s visitors or staff.
- A threat to visitors or staff within the CCG from terrorist or other potentially.

The aim of a site lockdown is to exclude or contain people by preventing entry, exit or movement of people on site. These arrangements will vary in complexity depending on the size of the premises and the scale of the emergency.

9.2. **Purpose, aims and objectives**

This policy and procedure has been developed to ensure that sufficient information is obtained wherever possible to determine whether the threat is a credible one or a malicious hoax and to make clear how staff need to respond.

9.3. **Limitations in a lock down**

The consequences of instigating a proportionate lockdown and the short, medium and long-term effect it may have on NHS services must be considered by G&W CCG management. Their decision to lock down must be underpinned by the legal reasons for doing so.

The accessibility of G&W CCG premises is often more controlled than a provider location, and therefore a lock down is less complicated (access to patients etc is not a consideration).

The CCG or the owner of any such G&W CCG premises has a right to refuse access to any of these premises. In this instance, if someone other than the owner (or a
tenant or a licensee) enters the premises having been advised not to, or is already on the premises and refuses to leave, they may be considered a trespasser and reasonable force may be used to prevent access or to remove them. If an individual enters the locked down premises or refuses to leave, they could be prosecuted under criminal law.

In the absence of the police, who are able to enforce a containment cordon, it will only be lawful for a G&W CCG to prevent exit of a significant number of people from its premises by utilising specific legislative provision. Even when these specific regulations can be used, specific tenets of the Human Rights Act 1998 must be considered – for example, a person’s right to liberty (Article 5) and an individual’s right to a family (Article 12). Without these regulations, it is likely that exit could only be prevented in relation to specific individuals in certain circumstances, which are likely to be limited to the following situations:

9.4. Planning a lock down

A lockdown is achieved through a combination of physical security measures and the deployment of security personnel.

There are three key elements that are crucial to locking down the CCG or part of the CCG:

- Preventing Entry
- Preventing Exit
- Preventing/restricting movement of people

The fundamental purpose of one or a combination of the above is to either exclude or contain staff, patients and visitors. The lockdown plan can be applied to achieve partial, progressive or full lockdown.

9.5. Levels of lock down

a) Full/Total Lockdown: This is the highest level and includes facility and perimeter security. A full lockdown is the process of preventing freedom of entry to and exit from either an entire NHS site or from a specific G&W CCG building. During a full lockdown, ALL perimeter doors are secured and NO ONE is allowed to enter or exit the facility. Security personnel or other designated personnel (designees) will be assigned to key entrance/exit points.

b) Partial Lockdown: A partial lockdown can be defined in a number of ways. In most instances, a partial lockdown is the locking down of a specific part of a G&W CCG site or a specific building or part of a building.

Other lock downs are Portable Lockdown, Progressive Lockdown, Controlled Lockdown, but considering the CCG occupies a non-complex small area, only the above two are deemed appropriate.

A lockdown should be used to ensure the safety and security of staff, patients, public, property and assets
9.6. Declaration of a G&W CCG lock down

The declaration will be made by the Chief Executive and/or his/her Deputy, or the On-call Executive or following a request from a Police Incident Officer. The declaration will be made after taking advice from the police or other emergency services. Where a decision needs to be made quickly and consultation would delay the implementation thereby posing a threat to the safety of visitors or staff, a decision to lockdown can be made without consultation. The CCG Management Team should be made fully aware of the reasons behind the decision and a Strategic Response Team (SRT) meeting convened to discuss the implications.

9.7. Initiation of lock down procedures

As soon as a lockdown has been called, staff should follow instructions by the Lock Down Marshalls or emergency services.

Lockdown procedures will be put in place using the following principles:

- Selected G&W CCG entrances will be put on “lock down”.
- All visitors will be denied access into the CCG.
- Visitors currently in the building will be instructed on the actions they need to take.
- Only essential employees (employees who have not been asked to stay at home) will be allowed access but must be in possession of their ID badge.

As soon as lockdown staff has been briefed on the incident details, they will need to go as quickly as possible to fulfil their roles. Action must be taken as quickly to secure the building. Any access controls should be utilised to speed up the process. A manual lockdown should be undertaken as quickly as possible.

9.8. Command and control

Where the reasons for CCG lockdown are based on criminal activity, strategic command will be led by a senior police officer who will coordinate the response. In extreme circumstances, e.g. a terrorist incident, it may be necessary for the police to take executive action in respect of the total incident.

9.9. Stand down

Only the on call Director or his/her deputy is able to instigate the stand-down authority which will be communicated directly to staff.

On stand-down all doors and barriers will be removed in an orderly fashion to enable The CCG to return to normal services as promptly as possible. Staff will remain on duty until instructed to leave or reassigned other duties.
9.10. Training

Training in lockdown procedures will be given to all Lock relevant staff. The lockdown training will be delivered by the LSMS/Security Manager (TIAA) in conjunction with the Emergency Planning Liaison Officer.

10 References

- Health and Safety at Work Act 1974
- Secretary of State Directions Nov 2003 Violence Against Staff
- Management of Health and Safety at Work Regulations 1999
- Police and Criminal Evidence Act 1984
- Children’s Act 1989
- Unfair Contract Terms Act 1977
- Occupiers Liability Act 1957
- Occupiers Liability Act 1984
- Health Service circular 1999/226 “Campaign to stop violence against staff working in the NHS: Zero Tolerance
- Health Service circular 1999/229 “Working together securing a quality workforce for The NHS: Managing violence, accidents and sickness absence in the NHS.
- CFSMS “Tackling violence against NHS staff” November 2003
- CFSMS “A framework for reporting and dealing with non-physical assaults against NHS staff and professionals” 2004
- Data Protection Act 1998, HMSO
- CCTV Code of Practice 2000, Information Commissioner
- NHS Security Management Services Security Manual Section 5 (CCTV)
- Human Rights Act, HMSO
- Records Lifecycle Policy.
### 11 Appendix 1 Procedural Document Checklist for Approval

**Procedural document checklist for approval**

To be completed and attached to any document which guides practice when submitted to the appropriate committee for consideration and approval.

<table>
<thead>
<tr>
<th>Title of document being reviewed:</th>
<th>Yes/No/Unsure</th>
<th>Comments/Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Strategy and Policy</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### A Is there a sponsoring director?

- **Yes**
- **Chief Finance Officer**

1. **Title**

   - Is the title clear and unambiguous?  
     - Yes

   - Is it clear whether the document is a guideline, policy, protocol or standard?  
     - Yes

2. **Rationale**

   - Are reasons for development of the document stated?  
     - Yes

3. **Development Process**

   - Do you feel a reasonable attempt has been made to ensure relevant expertise has been used?  
     - Yes

   - Is there evidence of consultation with stakeholders and users?  
     - Yes

4. **Content**

   - Is the objective of the document clear?  
     - Yes

   - Is the target group clear and unambiguous?  
     - Yes

   - Are the intended outcomes described?  
     - Yes

5. **Evidence Base**

   - Is the type of evidence to support the document identified explicitly?  
     - Yes

   - Are key references cited?  
     - Yes

6. **Approval**

   - Does the document identify which committee/group will approve it?  
     - Yes  
     - **Audit Committee**

7. **Dissemination and Implementation**

   - Is there an outline/plan to identify how the document will be disseminated and implemented amongst the target group?  
     - Yes  
     - Ebrief, On call pack, Corporate Induction
## Procedural document checklist for approval

To be completed and attached to any document which guides practice when submitted to the appropriate committee for consideration and approval.

<table>
<thead>
<tr>
<th>Title of document being reviewed:</th>
<th>Yes/No/Unsure</th>
<th>Comments/Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Strategy and Policy</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Please provide details.

### 8. Process for Monitoring Compliance

Have specific, measurable, achievable, realistic and time-specific standards been detailed to monitor compliance with the document?

**Yes**

Through SRT and annual security audit

### 9. Review Date

Is the review date identified?

**Yes**

March 2019

### 10. Overall Responsibility for the Document

Is it clear who will be responsible for implementing and reviewing the documentation i.e. role of author/originator?

**Yes**

Estates and Facilities Manager

**Director Approval**

On approval, please sign and date it and forward to the chair of the committee/group where it will receive final approval.

<table>
<thead>
<tr>
<th>Name</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Karen McDowell</td>
<td>7 March 2017</td>
</tr>
</tbody>
</table>

**Committee Approval**

On approval, Chair to sign and date.

<table>
<thead>
<tr>
<th>Name</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jacqui Burke</td>
<td>March 2017</td>
</tr>
</tbody>
</table>

**Signature**

[KM McDowell]

[J Burke]
## Appendix 2 Compliance & Audit Table

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Measurable</th>
<th>Frequency</th>
<th>Reporting to</th>
<th>Action Plan/Monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commissioner Security Standards</td>
<td>Security Audit</td>
<td>Annually</td>
<td>Audit Committee</td>
<td>Security Action Plan</td>
</tr>
</tbody>
</table>