Local Security Management
Policy & Procedures
HS18
(Includes guidance on dealing with Abuse, Bomb Threats, Siege Situations, Suspect Packages)

<table>
<thead>
<tr>
<th>Version</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date Issued</td>
<td>May 2012</td>
</tr>
<tr>
<td>Review Date</td>
<td>June 2015</td>
</tr>
<tr>
<td>Policy Author</td>
<td>Local Security Management Specialist</td>
</tr>
<tr>
<td>Approved by</td>
<td>Quality &amp; Governance Committee</td>
</tr>
<tr>
<td>Date Approved</td>
<td>15 October 2012</td>
</tr>
</tbody>
</table>
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>PART 1 – Local Security Management Policy</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Introduction</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>Strategic Objectives</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>The Role of NHS Protect</td>
<td>5</td>
</tr>
<tr>
<td>4</td>
<td>Responsibilities</td>
<td>6</td>
</tr>
<tr>
<td>5</td>
<td>How the Organisation Risk Assesses the Physical Security of Premises and Assets</td>
<td>12</td>
</tr>
<tr>
<td>6</td>
<td>How Action Plans are Developed and Followed Up as a Result of Risk Assessments</td>
<td>13</td>
</tr>
<tr>
<td>7</td>
<td>Training</td>
<td>13</td>
</tr>
<tr>
<td>8</td>
<td>Incident Reporting</td>
<td>14</td>
</tr>
<tr>
<td>9</td>
<td>Equality Impact Assessment</td>
<td>14</td>
</tr>
<tr>
<td>10</td>
<td>Monitoring Compliance</td>
<td>14</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Section</th>
<th>PART 2 – Local Security Management Procedures</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>Access Control</td>
<td>15</td>
</tr>
<tr>
<td>11</td>
<td>Bomb Threats and Suspect Packages</td>
<td>16</td>
</tr>
<tr>
<td>12</td>
<td>CCTV</td>
<td>20</td>
</tr>
<tr>
<td>13</td>
<td>Conflict Resolution Training</td>
<td>21</td>
</tr>
<tr>
<td>14</td>
<td>General Security – NHS Property</td>
<td>21</td>
</tr>
<tr>
<td>15</td>
<td>General Security – Personal Effects</td>
<td>22</td>
</tr>
<tr>
<td>16</td>
<td>Good Housekeeping Practices</td>
<td>22</td>
</tr>
<tr>
<td>17</td>
<td>Identification Badges</td>
<td>23</td>
</tr>
<tr>
<td>18</td>
<td>Impersonation</td>
<td>24</td>
</tr>
<tr>
<td>19</td>
<td>Information Security</td>
<td>24</td>
</tr>
<tr>
<td>20</td>
<td>Lockdown Procedures</td>
<td>25</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>------</td>
<td></td>
</tr>
<tr>
<td>21 Memorandum of Understanding</td>
<td>27</td>
<td></td>
</tr>
<tr>
<td>22 Reporting and Recording</td>
<td>28</td>
<td></td>
</tr>
<tr>
<td>23 Security Alerts</td>
<td>29</td>
<td></td>
</tr>
<tr>
<td>24 Siege or Hostage Situation</td>
<td>29</td>
<td></td>
</tr>
<tr>
<td>25 Staff Awareness</td>
<td>33</td>
<td></td>
</tr>
<tr>
<td>26 Other Policies and Guidance</td>
<td>33</td>
<td></td>
</tr>
</tbody>
</table>

**PART 3 – QUICK REFERENCE GUIDE**

<table>
<thead>
<tr>
<th>Appendix</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appendix A</td>
<td>Dealing with a Suspect Package</td>
<td>35</td>
</tr>
<tr>
<td>Appendix B</td>
<td>Checklist when Receiving a Bomb Threat</td>
<td>36</td>
</tr>
<tr>
<td>Appendix C</td>
<td>Impersonation/Suspicious Individuals</td>
<td>40</td>
</tr>
<tr>
<td>Appendix D</td>
<td>Guidance on Lockdown Procedures</td>
<td>41</td>
</tr>
<tr>
<td>Appendix E</td>
<td>Siege Situation – Initial Action</td>
<td>43</td>
</tr>
<tr>
<td>Appendix F</td>
<td>Monitoring Tool</td>
<td>44</td>
</tr>
</tbody>
</table>
Part 1 – Security Policy

1. INTRODUCTION

Wirral Community NHS Trust Board is committed to promoting and improving a safe and secure environment for those who work in or use the NHS so that the highest standards of clinical care can be made available to patients.

The Trust also aims to ensure that its policies will be compliant with the Human Rights Act 1998.

This policy is based on current directions from the Secretary of State for Health which is as follows:-

- Secretary of State Directions to NHS Bodies on work to tackle violence against staff and professionals who work or provide services to the NHS on 20th November 2003.

- Secretary of State Directions to NHS Bodies on Security Management Measures on 24th March 2004.

Any future changes to the above directions may supersede this policy.

Senior Managers of the Trust should take a leading role in promoting and developing a secure environment.

All Trust employees have a responsibility to ensure that security procedures are observed at all times.

This document sets out the framework for managing security within Wirral Community NHS Trust and will be underpinned by the procedures outlined in part II of this document.

2. STRATEGIC OBJECTIVES

The primary aims of this Policy are:

- The personal safety at all times of staff, patients and visitors as well as other employers and contractors.

- Protection of NHS property and assets against theft and damage.

- To ensure a safe environment in which the uninterrupted delivery of quality health care can be provided.

- To work in partnership with local agencies; e.g. police and local authority, for a safe and secure environment.
• Ensure that appropriate action is taken when security and the contents of this policy are breached.

• Ensure that in the event of a security incident escalating, any action taken is commensurate with action required to be taken in accordance with the Major Incident Plan and NHS Protect guidance on lockdown procedures.

• Ensure that breaches of security are reported in accordance with the Incident Reporting Policy.

• Ensure security of drugs, prescription forms and hazardous materials.

• To describe the remit of NHS Protect and the Local Security Management Specialist (LSMS) for Security Management within the NHS.

• To ensure the security of all personal information in accordance with the Data Protection Act.

3. THE ROLE OF NHS PROTECT

NHS Protect is part of the Counter Fraud and Security Management Service (CFSMS) and has overall responsibility for all policy and operational matters related to the management of security within the delivery of NHS services.

The aim of NHS Protect is a simple one - to protect the NHS so that it can better protect the public’s health.

NHS Protect is developing both proactive and reactive initiatives in relation to NHS security management work across the whole of the generic range of action, which includes:

• Creating a pro-security culture amongst staff, professionals and the public
• Deterring those who may be minded to breach security
• Preventing security incidents or breaches from occurring
• Detecting security incidents or breaches and ensuring these are reported in a simple, consistent manner across the NHS
• Investigating security incidents or breaches in a fair, objective and professional manner
• Applying a wide range of sanctions against those responsible for security incidents and breaches
• Seeking redress through the criminal and civil justice systems against those whose actions lead to loss of NHS resources
NHS Protect is committed to the delivery of an environment for those who use or work in the NHS that is properly secure so that the highest possible standard of clinical care can be made available to patients. This guidance is designed to reflect good practice which is used throughout the NHS.

NHS Protect has allocated an Area Security Management Specialist (ASMS) to each strategic health authority region to act as a link between NHS Protect and Local NHS Security Management. The telephone number for the ASMS for this region is 07717 301939

NHS Protect provides a National NHS Security Manual to be implemented across the NHS as a whole. This manual is a generic manual that will be used as a reference tool by the Local Security Management Specialist in the performance of their role at a local level. Sections of the NHS Security Manual have been referred to in this policy. It is a living document that will be updated and refined as Security Management initiatives are introduced and improved. This manual will be retained, maintained and updated by the Local Security Management Specialist.

4. RESPONSIBILITIES

Individuals

Chief Executive

The Chief Executive is ultimately responsible for the safety and welfare of staff, including protection from violence and aggression

Security Management Director

The Trust Board member with responsibility for security will be the Director of Finance and he will keep the Board informed of the major developments on security related issues.

The annual security report and plan will be signed and dated by the Security Management Director and a copy forwarded to NHS Protect in accordance with the Secretary of State for Health Directions 2003/4.

Directors

It is the responsibility of the Directors to:

(i) Disseminate this policy within the area of their responsibility.

(ii) Ensure the implementation of the strategy within the area of their responsibility by providing support and advice to their managers.

(iii) Co-ordinate security issues with other employers who share premises with Wirral Community NHS Trust.
Divisional Managers/Heads of Service

The Divisional managers maintain strategic responsibility for the provision of Security and for ensuring that this policy is cascaded and implemented within their division. Divisional managers are responsible for:

- Ensure local managers liaise with staff representatives as part of incident investigation and regular safety inspections to identify
- Ensure risks forwarded from their managers are controlled so far as is reasonably practicable and verify their entry onto the Risk Register.
- Liaise with relevant advisers to ensure that any planned service developments incorporate adequate control of exposure to security risks.

Service Leads

Service leads need to assess the impact of security within their department ensuring risk assessments are completed within their service area and recorded on the Risk Register.

When there are implications for safety and staff, they must ensure that action plans are developed where required, reviewed via the Divisional/Service governance meetings and managed in accordance with GP45 Procedure for Risk Identification and Management.

Service Leads are responsible for:

- Developing local arrangements to reduce the risks.
- Ensuring processes are in place to deal with any emergency situation.
- Implementing any necessary remedial action identified by incidents, audits or inspections.
- Liaising with controllers of premises where Wirral Community NHS Trust staff are based to ensure their safety in those premises.
- Ensuring that future job descriptions for all managers include, as part of their duties, the responsibility for security within their department.

Managers’ Responsibilities

All managers carry a responsibility for security. It is their job to see that the right policies, procedures and systems are in place in their local areas and that such policies are kept under constant review. They need to carry out risk assessments in relation to all significant hazards faced by staff and ensure they receive relevant instruction and training.
It is the individual managers’ responsibility to see that safe and secure environments are maintained and that all incidents are fully reported and that action is taken when necessary.

Managers should:

- Implement a procedure to record details i.e; make, model, serial number etc. of valuable or important property within their department/directorate. The Local Security Management Specialist can advise on methods to secure property.

- Ensure that arrangements are made to secure the department/directorate out of working hours together with the safe custody of keys.

- Ensure the setting of any security alarm or to protect the property out of hours.

- Ensure records are kept of all keys issued to staff in their department/directorate and reporting of all losses of keys to the Security Manager.

- Seek advice from the Security Manager to ensure that security is maintained within their Department/Directorate.

- Advise the Security Manager of any changes within their department/directorate that may adversely affect the security of premises.

- Ensure all staff employed within the NHS environment have an identification badge and when appropriate wear them.

- Ensure that all staff are made aware of this strategy and understand its content and their responsibilities.

**Local Security Management Specialist**

Locally, each NHS organisation is required under Secretary of State Directions to have access to an accredited Local Security Management Specialist (LSMS).

The role of the LSMS is to implement at a local level, the national policy for Security Management, and to work proactively and reactively with their NHS employers to ensure that staff are supported on Security Management issues and thereby reduce risks.

The LSMS has to undergo training, provided by NHS Protect, and achieve a level of accreditation.

Your Local Security Management Specialist is based at Old Market House, Birkenhead

Office telephone number: **0151 514 2888 Ext 1492**
Under a service level agreement with Wirral NHS Primary Care Trust until April 2013, the LSMS will also provide support for the management of security to all who work in NHS Primary Care in the Wirral area.

The overall objective of the LSMS is to “work on behalf of the local NHS to deliver an environment that is safe and secure so that the highest standards of clinical care can be delivered to patients.” This objective will be achieved by working in close partnership with staff, patients, their carers, NHS Protect and other stakeholders. The LSMS will aim to provide a comprehensive, inclusive and professional security management service for their NHS organisation, including independent contractors, and work towards the creation of a pro-security culture within the NHS.

A summary of the key objectives of the LSMS are:

- To comply with and implement the Secretary of State’s Directions for Security Management in the NHS.
- To become an accredited LSMS as assessed by NHS Protect and maintain this accreditation.
- To ensure that all NHS Security Management work is carried out within a professional and ethical framework as provided by NHS Protect.
- Ensure that all relevant stakeholders are involved in Security Management in the local NHS.
- To report to the Local Security Management Director on security management work locally.
- To ensure that strong links are maintained with NHS Protect and the ASMS.
- To lead on day to day work locally to tackle violence, harassment and abuse against NHS Staff, patients and carers, in accordance with the national framework.
- To maintain appropriate links with the local risk management process,
- To take steps to promote a pro-security culture at a local level.
- To ensure that security incidents/breaches are investigated, appropriate actions taken and to publicise the outcome, where appropriate, in accordance with guidelines issued by NHS Protect.
- To ensure that lessons are learnt from security incidents/breaches and preventative measures introduced to eliminate future occurrences, where possible.
- To encourage the reporting of security incidents/breaches, investigate these reports, assess risks, and implement preventative measures.
- To act professionally at all times, ensuring that a fair, objective and professional approach is taken at all times.
- To work towards applying a range of sanctions against those responsible for security incidents/breaches, being aware of the law as it applies to each incident/breach.
- To provide advice regarding the physical security of premises, proposed new premises, alterations to premises and assets.
- To maintain records of annual risk assessments showing action plans that are in place and changes that have been implemented.
• To work with the Local NHS and the National Legal Protection Unit to ensure that appropriate redress is sought against those who commit security incidents/breaches, including redress when a loss of resources has occurred.
• Ensure relevant information about potential security risks is circulated and all relevant staff alerted to the risk.

Health and Safety Advisor

The Trust Health and Safety Advisor and Local Security Management Specialist work closely together on violence and security issues. They will provide assistance to managers undertaking violence at work risk assessments and report to the Health, Safety and Wellbeing Group on the implementation of risk assessments by directorates.

Responsibilities of the Employee

Employees are expected to co-operate with management to achieve the aims, objectives and principles of the security strategy. Great emphasis is placed on the importance of co-operation of all staff in observing security and combating crime.

Staff should be aware of their responsibilities in protecting at all times, the assets/property of patients, visitors and Wirral Community NHS Trust. Where specific security procedures exist, staff must abide by them at all times. When staff know or suspect a breach of security, they must report it immediately to their manager or the Local Security Management Specialist.

All staff are reminded that it is an offence to remove property belonging to Wirral Community NHS Trust without written authority. Failure to seek authority from their line manager could result in disciplinary action or criminal proceedings being taken.

Staff are responsible at all times, for the protection and safe keeping of their private property. The Local Security Management Specialist will if requested, advise staff on the security of their property. Any loss of private property must be reported without delay. If private property has been stolen, then it is the owner's responsibility to contact the police.

Wirral Community NHS Trust will not accept liability for the loss of, or damage to private property.

All staff, official visitors and contractors working on behalf of Wirral Community NHS Trust are required to wear an approved security identification badge at all times unless medical or operational situations prevent this being possible.

Committees/Groups

Trust Board

The Trust Board has overall responsibility for ensuring compliance with health and safety statutory requirements.
For the effective implementation of this policy, the Chief Executive and the nominated directors require assurance that security management processes, procedures and policies are being effectively introduced and implemented within this organisation.

**Quality and Governance Committee**

The Quality and Governance Committee will:

- Review the findings and ensure implementation of recommendations arising from internal audits of Trust risk and security processes.
- Report to the Board on all aspects of quality, governance and compliance.
- Receive assurance that Wirral Community NHS Trust meets all relevant statutory and regulatory obligations in relation to quality, clinical governance and compliance through its reporting and monitoring structures
- Advise Wirral Community NHS Trust Board of all significant risks, areas for development and exceptional good practice, ensuring lessons are learned and shared

**Health, Safety & Wellbeing Group**

The Health Safety & Wellbeing Group will:

- Approve Local Security management policies
- Raise awareness of any significant Health and Safety risks within the organisation and ensure these are included in the risk register as appropriate.
- Receive regular performance assurance reports from all services including evidence of compliance against policies and standards
- Review the annual security report and risk assessment produced by the LSMS and escalate as required in line with GP45

**Divisional/Service Governance Groups**

Divisional/Service Governance Groups will:

- Discuss, agree and monitor action plans for risks belonging to their service.
- Ensure significant risks are recorded on the risk register
- Escalate risk issues in line with the Procedure for Risk Identification and Management GP 45
• Review incidents and local action plans that are implemented and lessons learnt post incident.

5. HOW THE ORGANISATION RISK ASSESSES THE PHYSICAL SECURITY OF PREMISES AND ASSETS

Risk Assessment by Heads of Division/Service Leads

a) Managers must give consideration to the potential risks faced by staff and members of the public, and the control measures that must be put into place to avoid or control the risks.

b) Having identified any hazardous situations for example following an incident, managers must determine whether existing controls are adequate or whether more needs to be done. This should be formally documented using the Risk Assessment Form to record the risks to which people are exposed. This assessment should take into account the risks inherent in the task, the environment, any other additional risks associated with the building or unauthorised persons and should consider any existing arrangements in place to manage the hazards faced.

c) Having assessed and recorded all the risks, which affect visitors and staff, in an establishment or when staff are away from the workplace and considered any existing controls in place, managers should consider whether these controls are sufficient or whether more needs to be done. Managers must take account of the extent that existing controls are being followed / implemented. In the event that further action is required managers are responsible for developing an action plan in conjunction with the LSMS. The completion of the action plan will be monitored at Divisional/Service Governance meetings and if requires escalated in line with GP 45

d) Information on the outcome of risk assessments must be fed back to staff as part of the risk assessment process

Staff should also be encouraged to seek advice / assistance if they are unsure about a situation or to report any problems / concerns via a line manager.

e) Having undertaken the risk assessment, recorded and implemented all necessary controls, it is important that risk assessments are monitored and reviewed at a frequency in line with the procedure for Risk identification and management GP45 and on the basis of any changes.

Risk Assessment by LSMS

a) The LSMS will additionally submit an annual security management report and plan to the Security Management Director. These documents will include the following information:
b) The annual security review and risk assessment of premises carried out by the LSMS using the ten principles of crime prevention as described in the Home Office ‘Passport to Crime Reduction,’ and the six principles for secured environments in the Association of Chief Police Officer’s guidance on designing out crime. All Community Trust premises and contents will be given a crime risk rating.

c) The annual security report and risk assessment will evaluate any actions taken by Service Leads and managers with specific reference to security incidents reported in the last 12 months.

d) The annual security plan will follow NHS Protect guidance and include clear objectives for the forthcoming financial year having regard to the current annual report and any foreseen changes to service. It will identify security priorities, timescales, and resources to carry out the plan, data to be collected, security strategies and links to the Major Incident Plan. The LSMS will ensure that security objectives are commensurate with current crime legislation, Home Office guidance and NHS Protect procedures and standards for provider services.

e) The annual security report will contain an evaluation of the security objectives based upon incident reports received and identify actions for improving and maintaining security based upon efficiency, effectiveness and value for money. A copy of this report and risk assessment will be presented to the Health, Safety and Wellbeing Group. An annual report identifying progress against the action plan and identifying losses will be prepared and submitted to the Security Management Director for agreement. Once signed the report will be submitted to NHS protect.

6. HOW ACTION PLANS ARE DEVELOPED AND FOLLOWED UP AS A RESULT OF RISK ASSESSMENTS

Risks identified via the annual security review by the LSMS and or service reviews will be managed in line with the procedure for Risk identification and Management. GP45. Where risks have been identified and added to the risk register, and further action is required an action plan considering possible risk treatments will be included with the risk on the risk register. The recommended minimum timescale for reviewing risks is detailed in GP45 however all risks should be reviewed when there is any change in the basis of the risk assessment e.g. any change in hazards or controls. Review and escalation of risks will be by the relevant group/committee dependant on the current risk score as outlined in GP45.

7. TRAINING

The organisation is committed to providing its staff with appropriate skills and knowledge to manage personal safety/security related issues.
Security training will be delivered by the LSMS according to the Trust Wide mandatory Training matrix. The management of mandatory training and core service level training is detailed in GP46 Learning and Development Policy

8. INCIDENT REPORTING

Any security incident whether actual or perceived that causes loss, harm or damage/the potential to harm Trust staff, assets, persons not in employment e.g. service users should be immediately be brought to the attention of a manager and recorded via the Datix incident reporting system (For further information about accident/incident reporting please refer to policy reference GP8).

Reports of theft and other criminal activity should also be made to the police and a police crime/incident reference number obtained and recorded on the Datix incident report.

9. EQUALITY IMPACT ASSESSMENT

In line with the Trust’s Equality Scheme, each procedural document should be screened by the manager responsible for its development, to consider whether there is an equality dimension or whether it is applicable to the Trust’s duty to promote equality. The equality screening process and any wider impact assessment should be recorded within the document.

As part of its development, this policy and its impact on equality have been reviewed as described above. The purpose of the assessment is to minimise and if possible remove any disproportionate impact on employees on the grounds of race, sex, disability, age, sexual orientation or religious belief. No detriment was identified

10. MONITORING COMPLIANCE

10. ACCESS CONTROL

Ideally access control measures that we use, and have confidence in, can help deter and prevent security related incidents.

They are designed to ensure that members of staff, patients and public only have access to areas they need to enter to do their job, obtain treatment or make enquiries.

Staff should wear identification badges, especially in secure areas.

Do not think that an NHS lanyard is good enough identification. It’s the badge that matters.

Staff should not lend access cards to others or wedge doors open and to be aware of the possibility of ‘tailgating.’

Tailgating is simply the act of following a person through an access controlled door after they have opened it using their access control card, key or by using a code controlled key pad.

If necessary staff should pause for a moment and secure doors behind them.

Anyone present on our sites without due reason should be requested to leave, having in mind own personal safety when doing so. On some sites assistance will be available, via on site security, to remove unauthorised individuals who are causing a nuisance and/or damage to those sites.

If unauthorised visitors refuse to leave then staff should take the most appropriate action, in a safe manner, to remove and/or summon assistance from security, porters, other members of staff, or the police as most appropriate in the circumstances.

Suspicious behaviour or unauthorised access to restricted or patient treatment areas should be reported to the manager of that area and an incident report completed.

Faulty access doors must be reported immediately.

All contractors and visitors requiring access to restricted areas of NHS premises should where possible be issued with identification badges that clearly show them as being authorised to access the relevant area. Local procedures will be in place that allows this procedure to be implemented.

Car Parking: NHS premises are private and there is no right of way. Car parking is allowed in specified areas and access is conditional on the owners or drivers of vehicles observing whatever safety regulations Wirral Community NHS Trust make to ensure the orderly flow of traffic, safety and security of all concerned.
The NHS accepts no responsibility for damage to or theft of vehicles whilst on NHS premises.

11. BOMB THREATS AND SUSPECT PACKAGES

(NB: In the event of an emergency; staff should refer to the quick reference guides at Appendix A, B and C).

This procedure is to support staff should there be a bomb threat or a suspect package (including possible chemical agents). Please note that this section is designed to be used (when appropriate) in conjunction with the Trust’s Major Incident Plan.

While the risk of an individual being caught up in a bomb related incident is low, bomb threats, be they real or hoax, could cause a great deal of disruption to the NHS.

The priority is to ensure that any such incident is managed effectively so that staff and visitors are not put at risk and to minimise the impact on the core business of Wirral Community NHS Trust.

Types of bombs:

It is important to be aware that bombs can easily be disguised to look like everyday objects. It might not therefore always be possible to recognise a bomb from its outward appearance. Some examples are:

- **Letter and Parcel Bombs** sent through the mail. They will generally contain only a small amount of explosives.

- **Anti-personnel bombs** for indiscriminate attacks on people, the aim being to kill or maim as many as possible. These can be nails or other jagged metal having a shrapnel effect.

- **Anti-property** for damaging buildings, especially dangerous in modern high rise buildings. They vary in size from a few kilograms to 200 kilograms or more.

- **Incendiaries** can be simple devices such as petrol bombs or more sophisticated including highly flammable and long burning materials.

General Guidelines – Bomb Threats and Suspect packages

A bomb or incendiary device is easily disguised, and is designed to cause damage by blast or fire. They can be concealed in a briefcase, handbag and flask or in the case of incendiary devices, in a cigarette pack, cassette tape or similar container. Litterbins and toilets have been favoured for depositing devices in the past. In recent times we have also seen the effects of suicide car bombers.

Report to a manager or Service Lead any object/person you see which you consider suspicious. Don’t hesitate or think twice about it. No one will criticise you for a false alarm. (Please use quick reference guide at Appendix ‘A’).
Do not touch or attempt to move a suspicious item.

Notify the police and switchboard immediately, giving your name, job title, your exact location and contact telephone number.

When calling the switchboard please remember to express the seriousness of the incident and the reason for calling and that action by a Director is needed immediately. The Director will consider implementing the major incident plan, as necessary.

The rota for the on-call Director is held at Arrowe Park Hospital switchboard, telephone number: 0151 678 5111.

Once the main switchboard has been contacted, consider if it is appropriate to contact the Communications Department who can assist in alerting as many members of staff as possible, for example:

0151 651 3905
0151 514 2311
0151 651 3961

Remain at a safe distance from the object and keep others away. Turn off radios / mobile phones within close proximity of the bomb or suspect package.

The police and bomb disposal will want to talk to you so make yourself known to the Emergency Services. Your first hand account of what you have seen is essential.

After a safe evacuation procedure from the premises, please ensure that all staff, contractors and visitors remain outside of the premises and a sufficient distance away from the building concerned. A minimum distance is 100 metres from the location of the incident but this will also depend upon police advice and other information available at the time of the event. Please be aware that fire evacuation assembly points may be too close to the property in question.

In the case of a lorry or a large van the police may set up a cordon 1000M away.

A check of all personnel should be conducted by managers or senior member of staff present to ensure that everyone has evacuated the premises.

**Staff should not go to their cars** nor remove their cars from the car park; this will take too much time and will lead to confusion.

**Do not let anyone re-enter the building** until instructed that the building is safe.

Consider the impact on the neighbouring properties and the need to inform them that a bomb threat has been received; they may then need to instigate an emergency evacuation from their property. The priority is the safety of staff and public and to minimise the risk of injury.
If you notice a package, about which you are suspicious, consider the relevant risk to both staff and patients within the premises and similar actions to those listed above in this section. If you have a serious concern about a package then, do not touch it and instigate the emergency evacuation procedure. Do not use mobile phones, personal radios or similar electrical devices in close vicinity of such suspect devices.

The person receiving the notification of a bomb, or similar alert, is the key to dealing with the incident and will be a key liaison for the police and LSMS with whom to make contact with. The details of the threat received, and its accuracy, are key to dealing with the threat. Copies of plans/drawings for each site should be kept in the Major Incident Plan cupboard.

A decision to re-occupy the building should only be taken once instructed to do so by the Police.

**Postal Bombs – Possible signs and appropriate action to be taken.**

Any one of the following signs should alert members of staff to the possibility that a letter or package may contain an explosive device.

- Grease marks on the envelope or wrapping
- Unusual odour such as marzipan or machine oil
- Visible wiring or tin foil, especially if package is damaged
- Envelope or package may feel heavy for its size
- Weight distribution may be uneven.
- Contents may be rigid inside a flexible envelope
- May have been delivered by hand from unknown source
- If a package, it may have excessive wrapping
- There may be poor handwriting, spelling or typing
- It may be wrongfully addressed or from an unexpected source
- There may be too many stamps for the weight of the package

Initial action for dealing with a package that may contain an explosive device:

- Put down gently and walk away from it
- Evacuate the immediate area and raise the alarm (*Immediate area may mean a room, department or building and will depend upon the size and type of building*)
- Inform the police via the 999 system
- Inform your manager
- Prevent anyone from re-entering the premises.
- Do not place the package into anything (e.g. water) or place anything on top of it
- Do not tamper with or open the package
- Make a description of the article and its location within the room (e.g. size, shape, lettering on it).
- Establish if possible, whether the person to whom the package is addressed is expecting the package
• Complete Trust Incident Report Form and forward a copy to the Local Security Management Specialist.

Dealing with telephone warnings of a bomb threat

Historically it is switchboard operators who most frequently receive telephone bomb warnings, but any member of staff with a direct dial facility might also receive a threat.

Terrorists often issue telephone warnings to organisations that would not be affected by the explosions (i.e. a third party). However, in all cases telephone the police immediately via 999 system with as much information as possible.

A checklist is provided at appendix ‘B’, to assist in gathering evidence. This form should be displayed prominently to reception staff and completed upon receipt of a bomb threat.

There are four key rules:-

• Keep calm
• Obtain as much information as possible for the caller – make notes.
• Keep the line open even after the caller has hung up.
• Report the call to the police and your manager / Service Lead

If you receive a threat about a bomb at an alternative address then you should:

• Contact the police immediately, by dialling 999, and inform them clearly and concisely, of the information you have received, use the checklist at Appendix ‘B’
• Attempt to get in touch with the premises to which the threat has been made in order for them to instigate their evacuation procedure.
• Contact the LSMS or a Director of the Community Trust to inform them of the threat you have received and the actions you have taken.

It is advised that service leads bring details of this policy to the attention of their staff and that copies be kept within key staff areas within their service function. Additionally it is advised that all receptionist staff within the primary care trust will receive a direct copy of this procedure, which should be kept by them, at all times, within their work area.

Any new receptionist staff, including bank staff, should receive a copy of this procedure, from their manager, at the commencement of their employment at the Wirral Community NHS Trust.
Internal Procedures – Dealing with telephone warnings of a bomb threat

Member of staff receiving call should notify:

- Police 999
- Manager / Service Leads
- Executive Director on call
- Start log of events (e.g. time calls received)

Role of the Senior Nurse / Manager of call

- Make a quick survey and if necessary arrange evacuation to a safe area
- Supervise at scene until help arrives
- In the event of an explosion, survey casualties, arrange call out of doctors, additional nurses
- Identify the casualties
- Liaise with the Executive Director and collate information

Chief Executive / Executive Director

- Put on stand by or activate the Trust’s Major Incident Plan depending on a threat or explosion.
- Take charge and control log of events
- Liaise with Senior Manager at the scene.
- Ensure that the Communication lead is briefed on developments
- Consider if need to make the Strategic Health Authority and NHS Protect are aware of the threat/incident.
- Ensure that other health services are put onto alert i.e. Accident and Emergency and local GP practices.
- Provide local knowledge of the site to the other emergency services.

12. CCTV

Wirral Community NHS Trust has external and internal cameras designed to safeguard staff, patients, and visitors. To regulate the use of cameras, Wirral Community NHS Trust operates to a CCTV Code of Practice made in accordance with the Data Protection Act. A copy of this guidance can be obtained from the Local Security Management Specialist.

CCTV recordings are strictly confidential and held solely for the purpose of detecting or preventing crime or to assist with improving safety. All requests to view or obtain copies of CCTV footage must be made in writing to the Local Security Management Specialist for investigation outlining reasons for request.

The only exception to this rule is that a police office may view CCTV recordings that are relevant to the investigation of a recent crime.

All requests will be forwarded to the Security Management Director for approval.
13. **CONFLICT RESOLUTION TRAINING (CRT)**

Divisional Heads will ensure that staff receive training in the recognition and management of challenging behaviour (*Conflict Resolution Training*) as defined in the training needs analysis for the organisation.

All core mandatory training is recorded centrally by the Quality and Governance Service. Quarterly monitoring reports are prepared for the Learning and Development Group to monitor attendance rates.

A national syllabus for Conflict Resolution Training (CRT) has been devised by the CFSMS and agreed to by the member staff side organisation representing NHS staff. This training must include the 10 objectives from the national guidance, which are for delegates to be able to:

- Describe common causes of conflict
- Describe two forms of communication
- Give examples of how communication can break down
- Explain three examples of communication models that can assist in conflict resolution
- Describe patterns of behaviour they may encounter during different interactions
- Explain the different warning and danger signs
- Give examples of impact factors
- Describe the use of distance when dealing with conflict
- Explain the use of reasonable force as it applies to conflict resolution
- Describe different methods for dealing with possible conflict situations.

A copy of the training handbook is held on the intranet.

Once a frontline member of staff has received initial one day training they will be eligible to attend refresher training once every three years.

14. **GENERAL SECURITY - NHS PROPERTY**

It is advised that all NHS premises should remain as secure as possible at all times, and allow public access to authorised areas only for the purposes of receiving healthcare. The public should not have access to staff only areas and managers should take appropriate measures to ensure that this principle is complied with. Ideally, entrances to restricted areas should display appropriate signs. For example: ‘STAFF ONLY’ or ‘AUTHORISED PERSONS ONLY.’

Public areas should have a minimum of concealed places; such areas require good lighting and to be constantly supervised.

Premises should be regularly checked during the working day and thoroughly checked prior to closing. All doors and windows should be secured.
During normal “out of hours” period it is expected that NHS premises will be alarmed and be locked in accordance with the local security policy in place for those premises. It is also expected that equipment and other assets of the NHS are made appropriately secure, when not in use by NHS staff.

Across all sites except Riverside and Port Causeway any issues with regards to alarms sounding will be attended by the external contractor employed to respond.

15. GENERAL SECURITY - PERSONAL EFFECTS

Within all areas of the NHS, staff are advised against bringing cash or personal belongings, in excess of their personal daily needs, whilst on duty, and that any cash and personal belongings should where possible remain with the individual at all times. If this is not possible then it is advised that all personal belongings and cash should be stored in an appropriately secure area, within the work place.

Wirral Community NHS Trust will not be responsible for loss of personal property, cash and belongings. Each service area is expected to take the most appropriate measures possible to ensure that work areas remain as secure as possible and that appropriate storage facilities are provided to staff.

Although the WCNT accepts no responsibility for the loss of personal belongings, staff are encouraged to report any loss of their property and co-operate in any enquiry which may result in connection with the loss.

Service leads/Heads of Service are encouraged to remind staff of the advisability of insuring personal property and that the NHS accepts no responsibility for its loss.

As with all security related issues the advice of the LSMS can be sought on appropriate security measures to be implemented within specific work areas to ensure the protection of personal belongings.

16. GOOD HOUSEKEEPING PRACTICES

Managers should encourage good housekeeping both inside and outside premises belonging to Wirral Community NHS Trust. This will reduce the opportunity for breaches of security to go undetected.

Senior staff, in all disciplines, have a responsibility to apply appropriate routine security practices in relation to NHS property and assets.

Breaches of agreed security practices must be brought to the notice of the LSMS and reported in accordance with the Incident Reporting Policy.

Registers shall be maintained of assets/equipment used within each service area.

The Service Head is responsible for ensuring that the register is updated on a regular basis and that regular audits of assets/equipment registers are undertaken. The responsible person should be clearly identified on the register.
Evidence that such actions are undertaken should be made available to the LSMS or the Community Trust auditors on request. The type of equipment included in the register shall be that which is attractive in terms of personal usage, portable and potentially vulnerable to misappropriation. Wherever practicable equipment should be permanently security marked and contain a unique asset identifier.

Managers responsible for equipment shall carry out a check of all items at least once per year. This should be carried out by the end of February. Any discrepancies shall be notified in writing to the Director of Finance and LSMS who may also undertake such other independent checks as considered necessary.

If at any time assets/equipment are known to be lost or misplaced then this should be reported, via an incident report, and notified to the LSMS.

Additionally any damage to the assets/equipment should also be reported using an incident form.

Service Leads/ Heads of Service are responsible for ensuring that staff do not use NHS assets/equipment for purposes other than their intended use. NHS assets exist for the benefit of the NHS and the treatment of patients; they should not be used for personal gain.

Within each service area, the responsibility for security management rest with the Service Head. Advice can be sought, at all times, from the LSMS. Good security management, and local security procedures, are the keys to ensuring that we keep the NHS secure and protect staff, patients and carers from adverse incidents.

Staff, at every level, have a responsibility to take steps to protect assets, patients, staff, visitors, carers and themselves, to prevent theft, fire, damage and waste and to bring to justice those who offend against the NHS and criminal law. All adverse security incidents, or near misses, should be notified, by staff, to their manager, an incident form and risk assessment completed and reported to the LSMS for investigation, action or advice.

All staff will be expected to co-operate in any enquiry into incidents particularly where losses by theft or otherwise, may be anticipated.

Please refer to the Accident/Incident Reporting Policy (Community Trust Reference GP8) for further advice.

17. IDENTIFICATION BADGES

All NHS staff are issued with identification badges, which must be worn at all times, when conducting their duties as an NHS employee. The identification badge should be in a position on their clothing so that anyone can see the badge and should not be hidden from public view, unless medical or operational situations prevent this being possible.

When off duty it is advised that NHS staff remove their identification badges from view, and keep them in a secure place.
Staff should only display identity badges issued and approved by the NHS. The use of imitation badges and insignia which has not been assessed by Health and Safety is not permissible.

Staff must report immediately to their manager any theft or loss of their identity badge and complete an incident report. Details of a missing identification badge should be circulated so that all members of the trust can be alerted.

18. IMPERSONATION

If a health professional is advised by a service user that they think they have been approached/visited by a person who claims to be a health professional, but is thought to be bogus, then the pathway at Appendix ‘C’ should be followed.

19. INFORMATION SECURITY

Any personal information e.g. patient or staff identifiable information or data, must remain secure at all times and only be used when it is needed and for the purpose it is being held.

Any paperwork containing personally identifiable information should be locked away when not in use and any computer systems should contain appropriate security measures to ensure that access is only permitted to those that need to gain access on specific approved grounds.

Computer systems should be logged / turned off when not in use for any period of time. Further information in the use and security of “personal information” can be obtained from the relevant Caldicott Guardian, the Information Security Officer within WHIS and/or your LSMS.

At all times Wirral Community NHS Trust employees must comply with the Data Protection Act when conducting Trust business.

During recent years there has been an increasing number of electronic access systems installed which require staff to present a card or fob to a reading device in order to gain access. The majority of these systems identify the card holder and the time of access to a building or area. This information is strictly confidential and held in accordance with the Data Protection Act, solely for the prevention and detection of crime and to ensure safety.

All requests to view or obtain a copy of access control or CCTV data must be made in writing to the Local Security Management Specialist outlining the reason(s) for the request.

Requests will be forwarded to the Security Management Director for approval.

Staff responsible for maintaining the security of data held on an electronic access system or closed circuit television system must not allow any other person to view the data base unless authorised by the Security Management Director.
The only exception is where access is urgently required by a police officer who is investigating a recent crime.

20. LOCKDOWN PROCEDURES

In the event of pandemic influenza or some other abnormal event, excessive demand may be suddenly placed upon the normal services that are available. It may become necessary to request a total or partial lockdown of some or all of the Trust's premises.

This may require

- Enforcement of additional access controls to limit non essential visitors.
- Closing some facilities.
- Restricted/controlled access to areas generally open to public visitors.
- Restricting access to where materials are stored.
- Restricting visitors to avoid spread of the virus.

Lockdown: A lockdown is defined by the NHS Security Management Services as the process of controlling the movement and access – both entry and exit of people (this includes NHS staff, patients and visitors) around sites or specific buildings/areas in response to an identified risk, threat or hazard.

These buildings will in the main be owned or leased by Wirral Community NHS Trust but in some cases may fall under the control of other organisations such as the Local Authority. In the latter case permission may be required from those organisations concerned.

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

It is important to note that in locking down a trust there are three key elements, that is; preventing the entry, exit and movement of people on a trust site or in a building or part of a building.

In preventing the entry, exit or movement of people, or a combination of the three, the main aim of implementing a lockdown is to either exclude or contain staff, patients and visitors.

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 trust site or a specific building or part of a building.

A partial lockdown can also be implemented when entry restrictions are placed on a specific building to control the flow of people into it – via identification checks for example. This is also known as ‘controlled access’ to a site or building.
On these occasions, the partial lockdown can also be characterised as being ‘static.’ For example; the partial lockdown is sustained at a specific part of a site or building and it remains there.

A decision to implement a partial lockdown will usually be the initial response to an incident. This response will help to ensure that identified critical assets such as personnel and property are protected.

**Lockdown Activation**

Following the Major Incident policy the incident commander may call for a partial or total lockdown of NHS premises within the remit of the trust.

**Lockdown Deployment**

Security guards, porters and dedicated staff will be assigned to relevant security duties.

These duties may include guarding specific areas, temporarily securing entrances, affixing additional signs and providing advice and directions to the public.

**Lockdown Maintenance**

It is anticipated that some staff will be released from their normal duties to assist with dealing with abnormal situations. Estates, and Housekeeping staff will be assigned to designated doors to maintain the lockdown and to give guidance and instruction to those who are attempting either entrance or exit. Printed information will be issued to these staff in order to reduce conflict and confusion.

CCTV and electronic access controls where fitted must be maintained and monitored at all times to provide accurate and up to date reports of all persons on site or attempting to gain access.

Normal porter services will continue to be maintained, staff being assigned to duties on a priority and need basis.

In the event of lockdown all persons entering a building should be in possession of a valid form of identity.

The Head of Capital Projects and Premises must be contacted if additional resources are required. The following is a list of companies who presently provide accredited security patrols and key holder services to this trust:

- Mitie Security………………………….Telephone number: 0151 423 5262
- Arrows Security Systems……………..Telephone number: 0151 609 0909
- MPS…………………………………..Telephone number: 07721 539 352
- Heritage Security……………………..Telephone number: 0151 639 0772
Lockdown Stand-down

Only the incident control commander is able to instigate the stand-down authority which will be communicated directly to Managers who will verify the instruction before taking any action.

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

A debrief will take place as soon as is practical with those staff who wish to take part. Further debriefs will be communicated using normal trust communication service after the event.

External stakeholders

Following instruction from the incident commander within the incident control room relevant assistance will be given to the Police, Ambulance and Fire Services depending on the priority need. Due consideration will also be given to other stakeholders such as County and Local Council Emergency Planning Leads. This again will be communicated from the incident commander under guidance from external incident management remit.

Mutual Aid

In order to prevent the possibility of individual services such as the walk in centre becoming either contaminated or over-run with casualties, the incident commander may give specific instruction to the lock-down team to concentrate resources to the area to assist and facilitate either temporary or permanent relocation of services.

Manual Lockdown

Doors which are not able to be locked automatically will have dedicated staff allocated to each area with the correct keys to physically lockdown the area.

In the event of a manual lockdown, security staff should be fully briefed as to their duties. A briefing sheet is provided at Appendix ‘D’

21. MEMORANDUM OF UNDERSTANDING – UNEXPECTED DEATH

The purpose of this protocol is to promote effective working relationships between the National Health Service (NHS), Association of Chief Police Officers and Health and Safety Executive (HSE). The protocol will take effect in circumstances of unexpected death or serious untoward harm requiring investigation by the police, or the police and the HSE jointly. Guidelines were published by the Department of Health in November 2006 to provide practical and pragmatic advice on the implementation of the Memorandum of Understanding agreed by the NHS with the Health and Safety Executive and the Association of Chief Police Officers.
The guidelines apply where a patient safety incident has occurred, resulting in unexpected death or serious untoward harm.

They cover the following areas:–

- When to refer a patient safety incident to the Police and / or HSE.
- How to conduct an investigation, including advice on how to preserve and assess potential evidence and safeguard it.
- How to communicate with the Police, HSE, patients, relatives and staff.
- The procedure to establish, conduct and manage an Incident Co-ordination Group, including guidance on who should represent an organisation.
- Model terms of reference and agenda for the Incident Co-ordination Group, including guidance on the issues that should be considered at the initial meeting.
- What information should be shared by the Police and HSE with Trusts.
- How to handle communications, including media coverage.
- There is no substitute for referring to the Guidelines which can be accessed at: the following internet address:–


22. REPORTING AND RECORDING

Staff should be encouraged to report anything they consider suspicious to their line manager or the Local Security Management Specialist.

All security incidents and near misses must be recorded using the Incident Reporting System Procedures.

In the event of discovering that an incident (resulting in a breach of security) has taken place, staff will take reasonable steps to remedy the situation immediately and must inform their Manager, the LSMS or the appropriate on-call Duty Manager, as soon as reasonably practicable.

A National NHS Security Incident Reporting System (SIRS) for recording physical and non physical assaults and the loss or damage of NHS property is operated and coordinated by NHS Protect. The LSMS will be responsible for transferring information from the incident report to the national database.

If a member of staff sees or suspects that a crime is taking place, they should (if appropriate) immediately contact the Police via switchboard or direct using 999. Wherever possible the member of staff should keep the situation under surveillance without endangering their own safety or that of others.
Whenever possible the LSMS should be informed, who will advise of the most reasonable course of action, as deemed appropriate to the circumstances.

At no time should a member of staff put their own safety, or that of others, in danger, and should only attempt to intervene if they believe that their own personal safety is not at risk.

23. **SECURITY ALERTS**

NHS Protect will issue Security alerts via the LSMS network when appropriate, to highlight individuals or circumstances that give cause for concern. The LSMS will distribute such security alerts within Wirral Community NHS Trust as is deemed fit to alert service managers and staff of risks that they may face. Due to the nature of such alerts it is necessary, at times, to put such alerts on restricted distribution in order to comply with the Data Protection Act and an individual’s right to confidentiality. Alerts will be distributed by the Quality and Governance Service.

24. **SIEGE OR HOSTAGE SITUATION**

*(In the event of an emergency, please refer to Appendix ‘E’ for quick reference guide)*

Any person held against their will by force or threat of force (expressed or implied) must be considered a hostage. The taking of hostages is used in an attempt to secure total control in order to gain compliance with the wishes of the hostage-taker(s) in order to bring about the hostages release.

Hostage taking is a serious crime defined in law as;

A person whatever his nationality, who in the United Kingdom or elsewhere,-

(a) detains any other person (‘the hostage’), and

(b) in order to compel a state, international governmental organisation or person to do or abstain from doing any act, threatens to kill, injure or continue to detain the hostage, commits an offence.

*(Contrary to: The Taking of Hostages Act 1982, Section 1).*

Confusion or mishandling of a hostage incident could lead to avoidable serious consequences.

Primary objectives during a hostage situation are to:

- Preserve life; and
- Maintain the safety of staff and the public.
Contacting the Police – Siege or hostage Situation

The taking of hostages is always a matter for the police, and every area of the United Kingdom has officers on call who are specifically trained in hostage negotiation techniques. The police must therefore be called using 999, as soon as possible. The staff member making this call should make it perfectly clear that there is a suspected hostage situation. At the same time the LSMS or in his absence the most senior member of healthcare staff available must be informed.

The LSMS or senior member of staff should ensure that the Director of Finance and Chief Executive are informed and kept updated as to developments. Where the situation includes threats of explosives or other hazards, the guidance given on dealing with bomb threats above must be considered.

The police will benefit from the following information where available:

- The exact location of the incident including access points;
- Details of the hostage-taker including clinical condition and events leading up to the incident;
- Details of hostages;
- A suitable rendezvous point for police arrival, where they will be met by appropriate personnel;
- Any known weapons or items being used as such; and
- Any known injuries to any party.

Primary Action – Siege or hostage Situation

The following provides guidance only until the arrival of police officers who, upon arrival, will take over the control of the situation. The first five to ten minutes of any hostage situation are critical to setting the stage for the subsequent outcome, and tensions will be highest at this stage. It must be understood that the police have overall responsibility for the incident.

Prior to the arrival of the police, no attempt should be made to enter into any form of discussion with the hostage-taker, unless failing to do so would place the hostage at greater risk. No negotiation should be undertaken and no requests granted. If confronted by the hostage-taker(s) it must be stated that you do not have the authority to grant any of their demands.

No attempt at intervention should be made whatsoever, if there is any doubt as to its success or places the safety of those concerned. No intervention involving the use of force must be used unless:

- Life is in immediate danger; and
- Forcible intervention has a high probability of success.
If possible and it is safe to do so, the situation should be carefully assessed (for example, through the use of CCTV) in order to determine:

- The number of hostages;
- Physical descriptions, especially of the hostage-taker(s);
- Any specific demands or statements. Make written notes. It is useful to keep a log of times and actions taken for the information of the police;
- Behaviour patterns;
- Types of weapons; and
- Any other potentially useful facts.

Steps must be taken to ensure that the police are contacted as soon as possible together with details of any action taken. This should be done in a quick, quiet and discreet manner out of sight and hearing of the hostage-taker(s).

Where possible, relevant staff should be directed to secure the location by establishing an exclusion perimeter around the incident site at an appropriate distance relative to the risk presented. This will prevent the accidental incursion of unwary staff, patients and visitors into the incident scene. The exclusion area should also ensure that the immediate access route to the scene is secure, unobstructed and preferably unobserved from the incident location.

All non-essential staff and mobile patients should be withdrawn from the area, ensuring that this is done in a manner that will not cause alarm to the staff themselves or exacerbate the hostage situation. If this cannot be done without risk of inflaming the incident, no action should be taken. Where practicable, staff and patients should be protected by the securing of doors to relevant areas.

Arrangements should be made for all calls into and out of the hostage area to be diverted to the switchboard and for dedicated lines of communication to be made available to relevant parties.

Consideration should be given to greater risks than those currently present (i.e. access to hazardous materials) and, where it is safe to do so, steps should be taken to prevent access.

**Secondary Action – Siege or hostage Situation**

Witnesses to the incident should be asked to remain close to hand in order to provide the best information to the police when they arrive. Consideration should be given to arranging suitable support, such as access to counselling services, for those who may have been traumatised by the incident.

Information held pertaining to hazardous materials and fire hazards present on the site should also be made available to the emergency services.

No one should talk to the media unless the police press officer, who would have obtained the agreement of the police senior investigating officer in charge of the incident, approves the text. The hostage-taker(s) may be listening and could react adversely to media attention.
LSMS or appropriate senior personnel should arrange for the communications manager and NHS SMS to be briefed on the incident and they will liaise with the police press office, as appropriate.

Ancillary Action – Siege or hostage Situation

Consideration should be given to the location of other buildings in relation to the security incident, and whether any action needs to be taken in respect of these (i.e. managing unwanted onlookers).

Appropriate personnel and medical records of all parties involved should be made available to the police upon request.

The notification of next of kin for those held hostage is a matter for the police, unless specifically instructed by them otherwise.

Post Incident Management and Review

As soon as possible after the event, a meeting should be convened between all the agencies involved and the LSMS. The purpose of this debrief is to learn from the experience and to afford the revision of local and national guidelines or procedures in the light of that experience.

Issues about abortion, genetic research, and animal rights along with the more common issues such as estrangement, insensitivity to human emotion, pain and vulnerability ensure that the healthcare setting is not immune from the possibility of a hostage situation. Avoiding the issue will not cause it to go away. The key to maintaining the safe environment that the law requires and healthcare workers have a right to expect, lies in planning, training and commitment.

Guidance for Staff – Siege or hostage Situation

The sudden occurrence of a hostage situation can cause fear and panic, but it is important to try and remain as calm and as rational as possible.

- If you need medication, ask for it;
- Otherwise, do not say or do anything that may put you or others at further risk;
- Do not lose hope and avoid an open display of despair;
- Initially, do not speak to anyone unless spoken to;
- Try to calm the hostage-taker;
- Do exactly what you are told and do not make suggestions;
- Try to appear calm but do not turn your back towards the hostage taker;
- Under no circumstances argue with the hostage-taker;
- Be observant, you may be released at any time;
- Expect noise and lights if a rescue attempt is made; and
- In the case of a rescue attempt drop to the floor and stay there until told otherwise by one of the rescuers.
Profile of the Hostage-Taker

Potential hostage-takers who are most likely to be encountered in a healthcare setting come from four groups:

The **criminal** who is either:

- in the process of committing a crime and try to use hostages to achieve their objective or to escape; or
- prisoner patient, who may have both the experience and propensity to carry out violent threats and be motivated by the desire to escape.

The **aggrieved person** who feels wronged by the system and considers that there is no way to address what they perceive is a legitimate grievance.

The **estranged individual** who is experiencing disruption or disintegration of a significant personal relationship with a loved one.

The **acutely mentally ill** who may be first diagnosed as such during or after a hostage incident;

**Political terrorists** must also be considered but their activity in a healthcare setting is generally considered as a low risk.

25. **STAFF AWARENESS**

Good training is essential for all members of staff and management must lead by example. Every employee must know **WHAT TO DO**, and what **NOT** to do if there is a need to search or evacuate an area.

All staff should be aware of their surroundings and be on the look out for suspicious behaviour, unusual packages or objects.

Each employee has a responsibility to exercise a duty of care in respect of NHS property they use during the course of their duties.

26. **OTHER POLICIES & GUIDANCE**

This policy should be read in conjunction with other Trust polices and guidance, examples include:

- Human Resource policies
- Lone Working Policy **(HS6)**
- Incident Reporting Policy **(GP8)**
- Withholding Care Policy **(GP3)**
- Counter Fraud and Security Management Service web resources ([www.CFSMS.nhs.uk](http://www.CFSMS.nhs.uk)),
- NHS Security Manual (held by the LSMS)
- Wirral Health Informatics Service (WHIS) Information Security and related policies that are applicable to the Trust
- CCTV Code of Practice.
- Risk Identification and Management (GP45)
- Fraud and Corruption (GP32)
Dealing with a suspect package that may contain an explosive device

It is important to be aware that bombs can easily be disguised to look like everyday objects. You are looking for an unidentified objects which:

- Should not be there
- Cannot be accounted for
- Is out of place
- Ownership cannot be established

Report any suspicious looking object to your manager or Service Lead.

Do not touch or attempt to move it.

Do not place the package into anything such as water or place anything on top of it.

Notify police & switchboard immediately (Switchboard Tel no: 0151 678 5111)

Give the operator the following information:

- Your full name
- Your job title
- Your exact location
- Your contact telephone number.

(a) Evacuate the immediate area and raise the alarm

(b) Remain at a safe distance having regard to police advice and other information available at the time of the event.

(c) Keep others away and restrict vehicles from entering the area.

(d) Do not transmit from a mobile phone or radio within close proximity

(e) Make a written description of the article and its location within a room (e.g. size, shape, lettering on it).

Assist police or bomb disposal squad at scene by providing as much information as possible about the threat and the layout of the area.
Appendix B

Quick Reference Guide

CONFIDENTIAL (When complete)

Check list for recording evidence of a bomb threat (or similar warnings)

Please listen carefully to the caller and record the details exactly as YOU hear them. Keep any notes you make of the message that you received, as well as this checklist, the Police will require copies of this information.

<table>
<thead>
<tr>
<th>Current date and time</th>
<th>Telephone number of person making the call (if known):</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date and time of call or threat was made:</td>
<td>Telephone number at which the call was received:</td>
</tr>
</tbody>
</table>

Details of the exact words spoken in the telephone message/warning

Try and ask the caller the following questions and records their answers

1. Exactly **where** is the bomb?

2. **When** is it going to explode?

3. **What** does the bomb look like?

4. **What** kind of bomb is it?

5. **What** will cause it to explode?

6. **Who** placed the bomb?

7. **Why** did they place the bomb?

8. Is there a code word? If Yes what is it?

Time telephone call ended:
Information about the call

Did the voice sound familiar?

Yes  
No

If so who did it sound like (eg a celebrity) ?

Where there any background noises such as :

- Animal noises
- Personal Address System
- Office Equipment
- Music
- Street noises
- Crockery
- Motor vehicles
- Factory Machinery
- House Noises (eg TV)
- Other Voices

Yes  
No

If you answered yes to any of the above, please provide additional details below, be as descriptive as you possibly can, alternatively add anything else that made the call distinctive.

Information about the Caller

Please consider the following issues about the caller and your assessment of him/her/them

Was the caller :  
Male
Female

Could you tell their age :

Yes  
No

Your estimation of their age(s) :

Could you tell their nationality :

Yes  
No

What Nationality do you think they have :

How was their command of the English Language

Good
Fair
Poor

Was their speech  
(Please tick as appropriate)

Fast  
Slow  
Distinct  
Distorted  
Stutter  
Clear  
Slurred  
Normal
Information about the caller continued

How was their Manner?

<table>
<thead>
<tr>
<th>Calm</th>
<th>Angry</th>
<th>Rational</th>
<th>Irrational</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Coherent</th>
<th>Incoherent</th>
<th>Emotional</th>
<th>Laughing</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Voice Characteristics**

<table>
<thead>
<tr>
<th>Loud</th>
<th>Soft</th>
<th>High Pitch</th>
<th>Deep</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Hostile</th>
<th>Pleasant</th>
<th>Drunk</th>
<th>Drugged</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Did they have an accent?

<table>
<thead>
<tr>
<th>English</th>
<th>Irish</th>
<th>Scottish</th>
<th>Welsh</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Asian</th>
<th>African</th>
<th>East European</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

If other Dialect or distinguishing accents please specify:

The delivery of the call, did it seem

<table>
<thead>
<tr>
<th>Spontaneous</th>
<th>or Read from a prepared statement</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Please detail any other information you observed/thought about the caller below, again be as expressive and descriptive as you can be:

---

**Information you provide in this checklist must reflect your own experience when you received this call, do not let others tell you what to say, it should reflect exactly what you experience.**

When completed this form will be taken by the police attending to the incident or by the Local Security Management Specialist of the PCT (LSMS).

Information given in this checklist will be kept confidential and will form part of the police investigation into the call you received. The Police will also want to interview you about the call you received.
Information about the person receiving the call

Your First Name: 
Your Surname: 
Your Job Title: 
Your place of Work (full postal address): 

Who do you work for: 

Your contact telephone number: 

Did anyone else overhear the content of the call: [ ] Yes [ ] No

If Yes please provide details: 

Time and date the police were informed: 

Did you phone the police or someone else: [ ] Yes [ ] Someone else [ ] 

If someone else please provide their details below: 

Details of the first person you informed that you had received this call: 

Full Name: 
Job Title: 

Address or contact details (if known): 

Signed: 
Please print your name: 

Appendix B - (Sheet 4)
Appendix C

IMPERSONATION / SUSPICIOUS INDIVIDUALS

If a health professional is advised by a service user that they think they have been approached/visited by a person who claims to be a health professional, but is thought to be bogus, then the following steps should be taken:

In the first instance, the service user should be advised to contact Merseyside Police on 0151-709 6010 so that any unnecessary delay in safeguarding the general public is avoided.

The member of staff should obtain the following information from the service user without delay.
- Description of the person/vehicle
- Name of bogus professional
- Employing agency
- Purpose of visit to include if they specifically asked to see a child/adult and if they named them correctly, e.g. “I have come to see Mrs Jones/baby Lewis.”
- Date and time of incident
- Details of client/patient involved

The member of staff should immediately report the incident to their Line Manager/WCT Manager on call, if out of hours, on 0151-678 5111.

The member of staff should complete an Incident Form within that working day and sent to Line Manager.

1. The Line Manager must discuss the situation with the Divisional Head of Service. Advice from Merseyside Police may be sought on 0151-709 6010
2. The Divisional Head of Service will circulate a memo to all the following by fax and email, giving a brief description of the person and details of their attempted visit – Heads of Service, LHD Leads, CAYPD, Director of Strategic Partnerships, Safeguarding Team (to include Designated Doctor/Nurse)

Divisional Manager/Head of Service will feed back to Line Manager on outcomes

Line Manager will speak with service user and update action/progress
Appendix D  Briefing for Security personnel in the event of lockdown

The following written guidance should be handed to security guards and read out at briefings.

During an abnormal event which places greater demand upon the delivery of NHS services than that which is normally warranted, the primary care trust will endeavour to continue normal service for as long as possible but it may become necessary to close some areas and concentrate resources where they will be most effective. The main aim of security in tackling an abnormal event is:

- The security of medical supplies.
- The security of staff, particularly frontline.
- The protection of the general public.

Stockpiles of Medicine

Dedicated members of staff may be assigned to accompany delivery drivers. Each vehicle must contain a mobile telephone or radio contact. Drivers may require the assistance of security staff with parking and delivery of vital drugs.

Drugs must be stored in a secure room which is protected by an alarm. Keys must not be left in the lock.

Protecting Staff

If a visitor is unable to obtain the medication they seek then security personnel should be mindful that this may result in a dispute with staff.

Disputes may be quickly resolved by making sure that all information about how to collect medication is readily available and easily understood.

In the event that a minor dispute cannot be resolved then a Manager should be notified immediately and the complainant advised to contact in the first instance the Patient Advice Liaison Service on telephone number: 0151 647 4251 or if a more formal complaint is received, the Complaint's Manager on telephone number 0151 651 0011.

If a dispute escalates out of control then the police must be contacted immediately and the assailant requested to leave the premises.

Ensuring queues are orderly.

Length of queues and waiting times can also cause frustration and security personnel should ensure that there is no queue jumping and that signs are not removed. Some events may require the formation of two queues.
It is crucial to the success of distributing emergency drugs that people can move through the defined queue system as efficiently as possible and that order is maintained.

**Regular checks should be made to ensure the following:**

- Are drug storerooms secure and keys removed?
- Are the alarms, CCTV and electronic access controls working?
- Are all personnel wearing clearly visible identification badges?
- Are the issue and assessment areas clearly signposted at all times?
- Are fire exits clearly signposted and kept clear at all times?
- Is there a telephone landline immediately accessible in the event that assistance needs to be summoned?
- Do you know the name of the ACP Manager and where that person can be contacted?

**Any breach of security must immediately be reported to the Local Security Management Specialist or in his absence the Estates Department**
### Siege Situation ~ Initial Action

**Remember: you and everyone involved is a potential victim or hostage.**

<table>
<thead>
<tr>
<th>Initial Action</th>
<th>For further advice refer to section:</th>
</tr>
</thead>
</table>
| 1. Immediately telephone 999  
Call out emergency service (e.g: police, ambulance, Or fire brigade). | 24                              |
| 2. Inform the senior manager on duty and switchboard. Ensure that the Chief Executive, Director of Finance and on call Director are notified. | 24                              |
| 3. Do not take unnecessary chances                                           | 24                              |
| 4. Try to prevent unwary staff, patients or visitors from accidental entry of the incident scene. | 24                              |
| 5. If possible withdraw all non-essential staff, mobile Patients, contractors and visitors from the area. | 24                              |
| 6. Arrange for telephone calls into hostage area to be diverted to the switchboard. | 24                              |
| 7. Try to contain the situation – consider if there are nearby hazardous materials and the need to secure other buildings in the vicinity. | 24                              |
## Appendix F

<table>
<thead>
<tr>
<th>Minimum requirement to be monitored</th>
<th>Process for monitoring (e.g. audit)</th>
<th>Responsible individual / group / committee</th>
<th>Frequency of monitoring</th>
<th>Evidence</th>
<th>Responsible individual for development of action plan</th>
<th>Responsible committee for monitoring of action plan and Implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duties</td>
<td>Review of the policy</td>
<td>Health Safety Wellbeing Group</td>
<td>Annual or in event of breach of security</td>
<td>Policy complies with NHS Protect guidance directly referring to all applicable standards</td>
<td>LSMS</td>
<td>Quality and Governance</td>
</tr>
<tr>
<td>How the organisation risk assesses the physical security of premises and assets</td>
<td>Annual Security Assessment</td>
<td>Accredited LSMS</td>
<td>Annual or if breach of security</td>
<td>Premises Security Assessments&lt;br&gt;Annual security report conforms to NHS Protect format</td>
<td>LSMS</td>
<td>Security Management Director&lt;br&gt;NHS Protect</td>
</tr>
<tr>
<td>How the organisation carries out risk assessments for the prevention and</td>
<td>Risks are identified and conveyed to staff so that 'post incident' lessons</td>
<td>Service Leads</td>
<td>Annual or if significant changes</td>
<td>Risk Assessments</td>
<td>Service Managers / Team leaders liaising when</td>
<td>Quality Patient Experience and Risk</td>
</tr>
</tbody>
</table>

HS18 Local Security Management Policy – Version 2
<table>
<thead>
<tr>
<th>Minimum requirement to be monitored</th>
<th>Process for monitoring (e.g. audit)</th>
<th>Responsible individual / group / committee</th>
<th>Frequency of monitoring</th>
<th>Evidence</th>
<th>Responsible individual for development of action plan</th>
<th>Responsible committee for monitoring of action plan and implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management of violence and aggression</td>
<td>Are learnt. Assurance reports to HSWE</td>
<td></td>
<td></td>
<td></td>
<td>necessary with LSMS</td>
<td></td>
</tr>
<tr>
<td>Timescales for review of risk assessments in relation to violence and aggression</td>
<td>Review of risks at Divisional Governance meetings</td>
<td>Divisional Governance meetings</td>
<td>Annually</td>
<td>Risk Flyers Lesson plan from essential Learning</td>
<td>LSMS</td>
<td>Quality and Governance Committee</td>
</tr>
<tr>
<td>How action plans are developed as a result of risk assessments</td>
<td>Discussed with relevant staff and seen to be effective and where appropriate policies amended</td>
<td>Appropriate Service Manager / Team Leader</td>
<td>Annual or sooner if significant changes</td>
<td>Risk Assessments</td>
<td>Divisional Heads / Managers of departments</td>
<td>Divisional Governance meeting</td>
</tr>
<tr>
<td>How action plans are followed up</td>
<td>Annual security plan</td>
<td>LSMS</td>
<td>Annual</td>
<td>Annual security plan is commensurate with annual security report and follows guidance from</td>
<td>LSMS</td>
<td>Security Management Director</td>
</tr>
<tr>
<td>Minimum requirement to be monitored</td>
<td>Process for monitoring (e.g. audit)</td>
<td>Responsible individual / group/ committee</td>
<td>Frequency of monitoring</td>
<td>Evidence</td>
<td>Responsible individual for development of action plan</td>
<td>Responsible committee for monitoring of action plan and Implementation</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-------------------------------------</td>
<td>------------------------------------------</td>
<td>------------------------</td>
<td>----------</td>
<td>---------------------------------------------------</td>
<td>-----------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>assessments at Divisional Governance meetings</td>
<td>Groups</td>
<td>Monthly</td>
<td>NHS Protect Meeting minutes</td>
<td>Service Lead</td>
<td>Quality Patient Experience and Risk</td>
</tr>
<tr>
<td>Arrangements for making sure Lone Workers are safe</td>
<td>Safe working practices follow guidance of Lone Working Policy</td>
<td>Relevant Service Managers / Team Leaders</td>
<td>Annual</td>
<td>Annual Security Report</td>
<td>LSMS</td>
<td>Security Management Director</td>
</tr>
<tr>
<td>How the organisation trains staff in line with the training needs analysis</td>
<td>Attendance Reports prepared for the Learning and Development Group Divisional Governance Groups via Summary Learning &amp; Development reports</td>
<td>Head of Nursing, Quality and Governance Divisional Managers</td>
<td>A minimum of four times a year</td>
<td>Attendance reports</td>
<td>Reviewed by Learning and Development Group and by updates in Quarterly Reports for E &amp; W</td>
<td>Attendance Reports prepared for the Learning and Development Group Divisional Governance Groups via Summary Learning &amp; Development reports</td>
</tr>
<tr>
<td>Minimum requirement to be monitored</td>
<td>Process for monitoring (e.g. audit)</td>
<td>Responsible individual / group/ committee</td>
<td>Frequency of monitoring</td>
<td>Evidence</td>
<td>Responsible individual for development of action plan</td>
<td>Responsible committee for monitoring of action plan and implementation</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>------------------------------------</td>
<td>------------------------------------------</td>
<td>------------------------</td>
<td>---------</td>
<td>-------------------------------------------------</td>
<td>-------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>reports</td>
<td>reports</td>
</tr>
</tbody>
</table>