Mersey Care NHS
NHS Trust

TRUST-WIDE NON-CLINICAL POLICY DOCUMENT

Policy and Procedure for the Management of Security Systems

Policy Number:	**SA29**
Scope of this Document:	**All Staff**
Recommending Committee:	**LSMS Security Meeting/ Group**
Approving Committee:	**Executive Committee**
Date Ratified:	**December 2015**
Next Review Date (by):	**December 2017**
Version Number:	**Version 3**
Lead Executive Director:	**Executive Director of Finance (Deputy CEO)**
Lead Author(s):	**Head of Safety & Security**

TRUST-WIDE NON-CLINICAL POLICY DOCUMENT

2015 – Version 3

Quality, recovery and wellbeing at the heart of everything we do

Mersey Care NHS Trust

TRUST-WIDE NON-CLINICAL POLICY DOCUMENT

MANAGEMENT OF SECURITY SYSTEMS

Document name	**POLICY AND PROCEDURE FOR THE MANAGEMENT OF SECURITY SYSTEMS SA29**
Document summary	To ensure a consistent approach to the assessment and management of security within Mersey Care NHS Trust.
Author(s) Contact(s) for further information about this document	**Head of Safety and Security** **Telephone: 0151 472 4071**
Published by Copies of this document are available from the Author(s) and via the trust's website	**Mersey Care NHS Trust** **V7 Building** **Kings Business Park** **Prescot** **L341PJ** **Your Space Extranet: http://nww.portal.merseycare.nhs.uk** **Trust's Website www.merseycare.nhs.uk**
To be read in conjunction with	• SA03: Policy & Procedure for the reporting, management and review of adverse incidents (including serious untoward incidents and near misses) • SA18: CCTV Policy • SD3: Policy and Procedure for lone working • SD05**:** Service users missing from an inpatient area • SD18: Policy for the recognition, prevention and therapeutic management of aggression and violence • SD20: Policy and Procedure for the Searching of service users, their Room Possessions, Lockers, Personal Property and Ward Area (Local Services) • SD22: Children visiting Mersey Care sites • SD32: Weapons in the Community Policy • HR05: Development and training of staff within Mersey Care • IT02: IM&T Security • Security Directions for High Secure Services
This document can be made available in a range of alternative formats including various languages, large print and braille etc	

Version Control:

Version History:		
Stage of document, e.g., Consultation Draft, Version 1	Confirm who document was circulated or presented to, e.g., Presented to the Executive Committee for Approval	23/11/15
Version 2	Following LSMS meeting 26th Nov removed Police clinical liaison meetings (see 6.1) as police liaise directly with managers	27/11/15
Version 3	Review format	30/11/15

SUPPORTING STATEMENTS

SAFEGUARDING IS EVERYBODY'S BUSINESS

All Mersey Care NHS Trust employees have a statutory duty to safeguard and promote the welfare of children and vulnerable adults, including:

- being alert to the possibility of child/vulnerable adult abuse and neglect through their observation of abuse, or by professional judgement made as a result of information gathered about the child/vulnerable adult;
- knowing how to deal with a disclosure or allegation of child/adult abuse;
- undertaking training as appropriate for their role and keeping themselves updated;
- being aware of and following the local policies and procedures they need to follow if they have a child/vulnerable adult concern;
- ensuring appropriate advice and support is accessed either from managers, *Safeguarding Ambassadors* or the trust's safeguarding team;
- participating in multi-agency working to safeguard the child or vulnerable adult (if appropriate to your role);
- ensuring contemporaneous records are kept at all times and record keeping is in strict adherence to Mersey Care NHS Trust policy and procedures and professional guidelines. Roles, responsibilities and accountabilities, will differ depending on the post you hold within the organisation;
- ensuring that all staff and their managers discuss and record any safeguarding issues that arise at each supervision session

EQUALITY AND HUMAN RIGHTS

Mersey Care NHS Trust recognises that some sections of society experience prejudice and discrimination. The Equality Act 2010 specifically recognises the *protected characteristics* of age, disability, gender, race, religion or belief, sexual orientation and transgender. The Equality Act also requires regard to socio-economic factors including pregnancy /maternity and marriage/civil partnership.

The trust is committed to equality of opportunity and anti-discriminatory practice both in the provision of services and in our role as a major employer. The trust believes that all people have the right to be treated with dignity and respect and is committed to the elimination of unfair and unlawful discriminatory practices.

Mersey Care NHS Trust also is aware of its legal duties under the Human Rights Act 1998. Section 6 of the Human Rights Act requires all public authorities to uphold and promote Human Rights in everything they do. It is unlawful for a public authority to perform any act which contravenes the Human Rights Act.

Mersey Care NHS Trust is committed to carrying out its functions and service delivery in line the with a Human Rights based approach and the FREDA principles of **F**airness, **R**espect, **E**quality **D**ignity, and **A**utonomy

Contents

1. PURPOSE AND RATIONALE

1.1 The Trust takes the security and associated safety of staff and people visiting its premises very seriously. It also recognises that it has a duty to ensure that its assets are managed effectively and held as securely as possible.

1.2 Compliance with the directions from the Department of Health and the associated Security Management Service (SMS) outlined in Secondary legislation (Statutory Instrument 3039/2002) underpins the Trusts approach to security management.

The policy is based on the following principles:

- staff and visitors to the Trust should at all times be as safe as possible and that risks to them from violence or theft should be kept to a minimum.
- each individual has a responsibility to take reasonable steps to ensure the safety of themselves and their own personal property, visitors to the Trust, and the Trust's property.

1.4 The Trust adopts the Home Office's Crime Prevention Ten Principles (see appendix 3) which are: -

- Target Hardening (Making targets more resistant to attack or more difficult to remove/ damage)
- Target Removal
- Removal of the means to Commit Crime
- Reduce the Payoff
- Access to Control
- Visibility / surveillance
- Environmental Design
- Rule Setting
- Increase the Chance of Being Caught
- Deflecting potential offenders from committing a Crime

1.5 The above will be included within security risk assessments and direct the work of the Local security Management Specialist in developing improvements and, managing individual security breaches.

2. OUTCOME FOCUSED AIMS AND OBJECTIVES

2.1 The purpose of this policy is: -

- To provide staff with direction and guidance on how to maintain the security of all staff, service users, carers, visitors estate and property.

- To outline the roles of key staff involved in the provision of security.
- To set the standards system / processes that should be used to manage and monitor security.
- To outline the required reporting arrangements
- To specify the risk assessment and risk management requirements
- To raise awareness that security and safety is the responsibility of each and every individual entering or working in the Trust.

3. SCOPE

3.1 This policy applies to all Trust staff and individuals visiting or using its premises. It will highlight roles of specific professionals who have an over-arching responsibility for the management and implementation of security systems, processes and procedures. Additional security procedures are required within the High Secure Services (HSS) provided by the Trust and these are covered under the High Secure Safety and Security Directions, the National and Local Clinical Security Framework and a bespoke local security manual.

4. DEFINITIONS

4.1 For the purposes of this policy the definition of security includes: -

- The systems, processes and procedures used to protect staff and individuals visiting or using Trust premises as well as Trust property and estate against abuse, theft, physical threat and damage.

- A security incident is any event that has breached security measures put in place by the Trust and led to there being threat, loss, damage, which could include theft, abuse to staff or trespass.

- A near miss security incident is where the safety systems agreed do not work or are not implemented i.e. failure to use alarms or lock windows.

4.2 The Trust identifies three forms of security: - relational, environmental and procedural. It recognises that they are equally important in enhancing the safety and well being of service users, staff and carers and visitors to the Trust. The above forms of security are mutually dependent on each other. The terms are used to mean: -

4.3 Relational Security - the use of therapeutic relationships to build trust with services users / carers. The use of social and therapeutic activities provides opportunity to reduce boredom and frustration thus limiting the potential for incidents of aggression and violence.

4.4 Procedural Security - the use of set systems by all staff to ensure that valuables are locked away, dangerous items removed and egress and

access to buildings (door security) is effectively managed. These procedures are based on national guidelines and best practice.

4.5 Environmental Security - includes the layout of the ward and how it lends itself to the therapeutic engagement and observation of and with service users including e.g. the type of locks, doors furniture used etc.

4.6 Information Security - includes the safe and secure storage and exchange of both clinical and non clinical information sent within and externally to the organisation. The systems used relate both to information stored and used electronically as well as hard copy documents.

5. DUTIES

5.1 Local Security Management Specialist (LSMS)

5.2 Mersey Care NHS Trust has a number of accredited LSMS Practitioners within each clinical division who each provide: -

- Security advice and guidance to individuals and teams
- Expertise in facilitating investigation to enable prosecution to occur.
- A link with the national Security Management Service
- A resource to liaise with external agencies such as the Police and Crown Prosecution Service (C.P.S.)
- Supervision to security leads within clinical services.
- Coordination and implementation of the 'violent patient' marker system
- Proactive security risk assessments

In addition the LSMS are responsible for: -

- Facilitating security risk assessment following theft / violence (see appendix 2)
- Attending clinical meetings to provide a security perspective regarding the management of specific high risk people. Within High Secure Services Clinical Liaison Nurses attend clinical meetings.
- Collating security data and reporting internally and externally as agreed.
- Producing an annual report on security arrangements on behalf of the Trust Board which is shared with the Counter Fraud and Security Management Service.
- Managing the implementation of the lone worker device system.
- Facilitating police liaison meetings across the organisation.
- Monitoring trends regarding security incidents and implementing remedial action

5.3 Each LSMS is allocated to a specific area of the Trust i.e.: -

- Local Services
- Secure Services

5.4 They are the key point of contact for planning, analyzing, assessing and developing security arrangements in the organisation.

5.5 Security Management Director (S.M.D)

5.6 This role is a mandatory one, as outlined by the Counter Fraud and Security Management Service (C.F.S.M.S) and is responsible for ensuring that a strategic approach to improving the security within the organisation is taken. This role is currently undertaken by the, Executive Director of Finance who will: -

- Report serious security breaches to the board and follow up actions taken.
- Report on security provision, risks identified and management strategies used to enhance safety to the Trust Board and Quality Assurance Committee.
- Provide supervision and guidance to the LSMS, agreeing the security work plan annually.
- Monitor the number and type of security breaches, analyse for trends and consider the appropriateness of the management arrangements that are in place and how they can be improved.

5.7 Non Executive Director

5.8 As per C.F.S.M.S the Trust has a Non Executive Director who takes a special interest in the area of security, they will: -

- Attend appropriate security meetings and monitor the work of the accredited LSMS and SMD
- Discuss security arrangements within the Trust at Board level.
- Monitor the implementation of agreed actions plans.

5.9 Executive Director

5.10 The Executive Director of Finance is responsible for ensuring that the guidance set out by NHS Protect is adhered to within the trust and for reporting on an annual basis security issues to the trust board. This will be undertaken as part of the Health and Safety annual report. They are also accountable for ensuring the security issues are considered when new developments are being planned and developed within the organisation.

5.11 Divisional Service Directors/Departmental Heads of Service

5.12 Each Divisional Director/Head of Service has a responsibility to consider the safety and security of their staff by: -

- Ensuring that the LSMS is involved in reviewing security arrangements when services / environments are changed.
- Considering security as a priority issue and monitor locally the number of security incidents that take place and agreeing the remedial action to be followed.
- Monitor staff adherence to this policy i.e. that all staff wear name badges.
- Delegate a member of staff to take a lead on security and liaise with the LSMS, this will normally be the same person who takes responsibility for risk.
- Report security breaches to their security lead and at their governance meetings to ensure appropriate action is taken.
  Identify security risks and ensure they are monitored via the use of the services risk register,

5.13 Divisional Risk / Security Leads

5.14 Each Division will have one nominated individual who will take responsibility for: -

- Developing, in association with the LSMS, local Lockdown Protocols within each service.
- Monitoring completion of annual security assessments.
- Raising security issues within divisional governance meetings.
- Implementing this policy locally.
- Liaising regularly with the LSMS to seek advice and guidance.

5.15 Ward/Departmental/Team Manager (Managers)

- All staff (including bank, agency and contractors, students and others) must be made aware of the security policy / procedure by the ward manage/departmental/team manager on local induction / introduction to the ward or work area.

- Managers should receive information on any new problems within the security procedures and identify in association with colleagues the remedial actions required and take responsibility for ensuring the actions are implemented.

- Managers must ensure that their staffs wear identification badges at all times.

- Managers must ensure that all service users, carers and contractors, students and others receive information about the rationale for the procedures outlined within this document and how they operate which includes how they can ask for help entering and leaving the ward or work area.

- Within HSS there is access to both the national and local clinical security framework as well as mandatory security induction training for new starters.

5.16 Individual staff members

5.17 Each member of staff has a right and a responsibility to help keep themselves and their colleague's safe by: -

- Reporting all security breaches /incidents via the adverse incident management process.
- By adhering to all aspects of this policy and other associated ones.
- Attending recommended training.
- Remaining vigilant and asking unknown people why they are on the premises and to offer if they can help and assistance to ensure they are in the right place at the right time for the right purpose.
- Wearing their identity badges at all times.
- Within HSS staff will use the 5 x 5 security intelligence /incident reporting system is used.

5.18 Temporary or Agency Staff, Contractors, Students or Others

5.19 Temporary or agency staff, contractors, students or others will be expected to comply with the requirements of all Mersey care NHS Trusts policies and procedures, applicable to their area of operation. They will be informed of their responsibilities on induction or in the case of contractors on the first day they commence work with the Trust.

5.20 Estates Department

5.21 The Facilities and Estates Department is required to inform the LSMS of planned structural changes to a department and request that the LSMS provides guidance during the planning process to ensure that security issues are considered explicitly.

5.22 Within HSS there is a High Secure building design manual which covers design, over-arching principles and technical specifications. This document will direct any changes made to the environment.

5.23 PROCESS

Our policy is to;

- Undertake a risk assessment in relation to a procedural, environmental, relational security issue.
- Undertake security risk assessments - procedure should highlight frequency of these
- Undertake a re-assessment following a security breach
- Produce plans in place for improving, maintaining etc. security
- Liaise with the police on matters of security
- Prosecute when relevant to do so
- Collect incident data
- Train staff
- Produce information
- Monitor trends
- Learn from incidents

5.24 Risk Assessment

5.25 This section outlines the organizational approach to the risk assessment and risk management of security.

5.26 a. Annual Security Risk Assessments (See appendix 1)

5.27 A security risk assessment should be undertaken within each clinical/work area on an annual basis that considers the following: -

- Safety of service users and staff in relation to the prevention and management of violence and aggression
- Safety of property from theft, damage
- Safe storage of medication and medical devices
- Safe storage of personally identifiable information
- Control of access and egress to the department and usage of an appropriate and agreed reception procedure.
- Use of the agreed Search Policy (ward areas only)
- The number of people undergoing security training as per the agreed training programme.
- Control and prevention of prohibited items entering the department i.e. alcohol and illicit substances, knives, lighters etc.

5.28 The allocated LSMS will co-ordinate and facilitate the implementation of the assessments process.

5.29 Each Division/Department must have a system for monitoring the completion of security risk assessments and implementation of actions relating to the findings.

5.30 High Secure Services will undertake security assessments as part of the Prison Services annual audit.

5.31 None clinical areas should be audited every three years unless they are deemed to be high risk from the perspective of incidents of violence, theft. Adverse incident data will be used to identify none clinical areas that are deemed to require increased monitoring. Non clinical areas in HSS are incorporated into an ongoing security audit processes as well as being covered by the annual prison service audit.

5.32 b. Assessment following a security breach

5.34 All staff have a duty to report a crime. Once a crime has been reported, the LSMS must be informed (within 24 hours) so that they can ensure a security risk assessment is undertaken either by themselves or by an agency of their choice i.e. Crime Prevention Officer, Merseyside Police.

5.35 This will consider how security and safety can be improved and the actions staff must take. It will also consider the likelihood of a similar incident and prioritise certain actions (See Appendix 2) Issues requiring immediate action will be reported to the relevant line manager. The risk register will be used to monitor identified security risks and the Trust response to these. Any security issues assessed with a risk rating of 15 or over will automatically be escalated to the corporate assurance framework for monitoring by the Trust Board

5.36 c. Capital Projects

5.37 When a new building is being developed or an exiting building is being re-modelled, the LSMS must be involved to undertake or commission a security risk assessment which will: -

- Provide advice and guidance on how the changes will affect the security of service users, carers, staff, visitors and property.
- Provide ongoing direction as to the required security measures during the period that the building work is being undertaken to ensure that the security and safety of individuals and the environment is maintained.
- Identify the security systems / processes that should be in operation within the reconfigured / new building.
- Undertake a final security risk assessment as part of the end stage project management arrangements.

5.38 Within Secure Division (i.e. High, Medium and Low Secure Services), guidelines are available which specifically direct the standards to which work should be undertaken.

5.39 Action Plans

5.40 Recommendations made from risk assessments should be collated into an action plan. Where local management of the security risk is required key responsibility for implementation should be allocated to the relevant service management team. The governance framework within the service will provide a structure to monitor the implementation of the recommendations .Risks in relation to none / or delayed compliance will be entered onto local risk registers.

5.41 The LSMS will monitor the implementation of locally implemented action plans on a 6 monthly basis and advice on the management of actions that are not implemented or delayed.

5.42 A corporate action plan will be developed and managed by the LSMS in response to recommendations that need to be undertaken across the Trust and / or require corporate funding. Risks associated regarding none / delayed compliance will be reported bi annually at the Health and Safety Committee and entered on the corporate risk register.

5.43 Maintaining Safety

5.44 It is essential the Trust clarifies the behaviour that is acceptable within the organisation to all services users, staff, carers and visitors. Staff should also be aware of the approaches to be used in order to enhance the safety and security of themselves, service users and visitors. This includes: -

- Informing workmen visiting wards / departments of the safety standard set on the ward/work area i.e. alarm systems; safety of tools and how to access and egress the department via the use of a standard system and package of information.
- Within HSS MSU and LSU workmen and contractors are escorted.
- Displaying posters in all clinical and non clinical areas raising awareness of behaviour that is unacceptable.
- Encouraging all staff to question people who are not wearing identity badges to clarify if they have a legitimate reason to be in the building.
- Agreement between the LSMS and Management of Violence and Aggression Department regarding protocols to be used for responding to violent incidents
- Stopping, reducing or controlling access to Trust premises for visitors who abuse / threaten staff or cause significant damage.
- Meeting the standards required by the relevant policy where the removal of potentially dangerous items from service users/carers is necessary for the protection of self or others. .

- Staff awareness of the policy that is in place which identifies the standards required for searching service users / carers.
- Ensuring all buildings providing clinical interventions have an agreed protocol for responding to violent / abusive incidents.

5.45 Building Security

- All thefts / burglaries to property should be reported via the Adverse Incident Process so that the incident is logged and trends monitored.
- All buildings / departments should have a named person who is responsible for coordinating the security of the area i.e. Site Manager.
- Buildings which are not managed / occupied over 24 hours should be alarmed and linked to a contracted security provider.
- Each building will have clear and official signage regarding the behaviour acceptable within the area and sanctions used if it is breached.
- All areas providing 24 hour care / services should have access to security systems over a 24 hour period which includes a reception facility.
- Staff finding that an individual does not have a reason to be on Trust premises should: -
    - Consider asking them to vacate the premises.
    - Call for assistance from the Police.
    - Call for assistance from Security Services
- A policy should be in place that identifies the standards required for use of CCTV within both clinical and non clinical areas of the Trust.

5.46 Property Security

- All wards and departments should display disclaimer notices regarding the level of responsibility the Trust can take regarding personal items.
- Each clinical area should have a safe, to store service users' valuable property i.e. money / jewellery.
- Each service user should have access to an individual lockable draw / cabinet.
- Valuable property / money handed to ward based staff will be documented and the service

user (or their nominated deputy) will be provided with a receipt of the property to be stored. Items for safe keeping should not be stored on ward areas for more than 2 working days. Valuable item such as phones, rings / money should be stored on a longer term basis in the cash office or returned home.

- All Trust property deemed to be valuable and at risk of theft should be identified using an authorised security identification product such as 'Smart Water'.
- All car parks should display signs which identify the level of the Trust's responsibilities for cars parked.

5.47 Information Security

- To ensure the Availability: that is, ensure that assets are available as and when required adhering to the Trusts business objectives
- To preserve integrity: that is, protect assets from unauthorized or accidental modification ensuring the accuracy and completeness of the Trusts assets
- To preserve Confidentiality: that is, protecting information from
- Unauthorized access and disclosure.

- Trust Staff are bound by the confidentiality and security policies set by the NHS, and by the common law duty to maintain confidentiality Concerning the data and information you use as part of your everyday work within the NHS.

- Although it is recognized that Incident reporting may occur via the service desk in order to ensure that the incident is logged and trends monitored the incident should also be reported via the Adverse Incident Process.

5.48 The IT02: IM&T Security Policy contains a detailed description of the requirements for staff.

6 Police Liaison

6.1 The Trust contributes to the joint funding of a Police Constable (PC) who acts as a specialist Mental Health Liaison Officer between Mersey Care and Merseyside Police. Their principal role is to develop, policy and systems that help in the prevention, detection and prosecution of crime. The PC is based in the Public Prevention Unit, Merseyside Police. They also act as a central resource to aid in the coordination of police activity. The Police Liaison Officer can help clarify the rationale for a police response and provide expertise to neighbourhood police on action that should be taken.

6.2 The work of the Police Liaison officer is coordinated jointly by line managers within the police service and the LSMS for Local Services. The police Liaison officer will be invited to LSMS meetings to provide a mutual understanding of each others roles in:

- Monitoring how crimes are being investigated and prosecute
- Considering general security risks and how they can be managed
- Planning and Implementing security improvements

6.3 **Personal Responsibility**

6.4 Identification

6.5 It is essential that each staff member ensures that they have access to and wear a current Trust personal identification badge (containing a photograph of the individual) at all times. This allows them to be recognised by colleagues as a Trust employee and therefore provides them with a rationale to be on Trust premises. It also allows visitors to identify staff and therefore seek help and guidance from them. Lost or stolen name badges should be reported to the staff member's line manager and an incident report completed.

6.6 Care of Personal Property

6.7 Staff are responsible for the safe and secure management of their personal property and therefore should keep the property that they bring to work to a minimum both from a value and amount perspective. Where lockers and secure cabinets are available, staff should use them to keep their property safe.

6.8 **Reporting of Incidents**

6.9 All security breaches should be reported by the individual who first identifies them using the Trust's adverse incident reporting system.

- Where a crime is deemed to have been committed, the Police should be informed and requested to commence an investigation.

Where a building needs to be secured, the Estates Department should be informed immediately to provide remedial action.

- Where service users, carers, visitors and staff are deemed to be at risk, the Manager of the area should be informed who will clarify the actions that need to be undertaken to enhance safety. They will, where appropriate, seek advice from: -

    - Head of Quality & Risk
    - Local Security Management Specialist
    - Safety Adviser

- Each security incident should be reported to the LSMS within 24 hours of the incident occurring.

6.10 If IT equipment is stolen and potentially contains confidential material The Data Protection Officer should be informed.

6.11 Details of the work undertaken by contractors employed by the Trust With regard to estate maintenance and management to correct property damage should be collated and monitored by the LSMS against number and type of incidents reported with the aim of identifying gaps in incident reporting.

6.12 Sanctions

6.13 The Trust will consider the use of sanctions when an individual breaches its security measures, these will include: -

- Involvement of the Police.
- Sending warning letters regarding the unacceptable behaviour and highlighting the potential future involvement of the Police.
- Prevention of people entering Trust premises.
- Reduction / monitoring of visiting arrangements.
- Implementation of individually developed behavioural contracts

6.14 It is essential that sanctions used are proportionate and appropriate, respecting the human rights and responsibilities of the individual and take into account their mental health and physical safety.

6.15 Prevention of people entering Trust premises

6.16 Where a visitor to a clinical area has been deemed to have caused violence or abuse or they are suspected of bringing prohibited items into the unit, staff have a responsibility to consider how this incident will

be prevented from re-occurring. The following action should be undertaken: -

- The individuals should be warned about their behaviour verbally and in writing.
- The individuals should be informed that a future re-occurrence of the same or similar behaviour may lead to them being prevented from entering the building for a set time period which will depend on the severity of the incident and past history of the individual.

6.17 When preventing an individual from entering a clinical area, staff need to recognise that this may lead to the human rights of the individual and or the person they are visiting being infringed. Therefore the followings must be ensured: -

- The time relating to the sanction is limited to the shortest possible period.
- Provision of other forms of communication i.e. telephone, letter is made available.
- Documentation is made of the behaviour that has led to the sanction being implemented.
- Alternatives are considered i.e. supervised visiting.
- All individuals subject to sanction will be informed that they can use the Trust Complaints Procedure to raise any concerns.

6.18 It is important that the sanctions used are seen as being proportionate to the level of the incident. Legal advice can be sought on individual cases where the human rights of an individual may potentially be breached.

6.19 The Trust supports the involvement of the Police in the investigation and where appropriate, the prosecution of the perpetrators of crime. Trust Managers will actively help staff in reporting crimes against them to the Police.

6.20 Training

6.21 Staff familiarisation of the role of the Local Security Management Specialist is provided by the Personal Safety Service as part of the delivery of their training courses. Training is aimed at: -

- Raising the awareness of staff regarding their personal responsibility in creating a safe and secure environment.
- Clarifying the role of key people in the Trust who are responsible for security.

- Providing information on how and what sanctions can be used to help deter potential perpetrators of crime.
- Outlining the need to and importance of reporting security breaches.

6.22 Services can request security training session from the LSMS that are based on their own particular security needs. This will be facilitated as capacity allows.

6.23 Whilst the above has provided guidance on the training that is available, further specific detail can be found in the organisational training needs analysis which is incorporated within the Learning and Development Policy.

6.24 Key Access – inpatient units

6.25 Staff members working on inpatient units must attend a training session held by either the LSMS or nominated deputies prior to accessing keys/fobs. These sessions will be held regularly throughout the Trust and will last for approximately 45 minutes. The contents will include: -

- Prevention of tailgating
- Responsibilities of a key holder
- Removal of access to key, if breaches occur.
- Consequences of services users leaving the ward without permission.
- Role of ward security in preventing and managing risks

6.26 Coordination of Security Contracts

6.27 From time to time the Trust may require the contracted services of an external security provider. An accredited LSMS should manage a database of all security providers and participate in the coordination of contracts and adherence to agreed standards. The role of security guards employed via a service level agreement must be clearly identified to ensure that roles are delivered professionally and in accordance with the requirements of the Trust.

6.28 Management of Security Alerts

6.29 Then national Security Management Service shares alerts related to individuals who are known to be violent / abusive to Health Care staff or have a history of other types of crime (theft / fraud) against the NHS and its staff.

6.30 The LSMS will review each alert as it is received and decide if it is suitable for sharing within the Trust; issues taken into consideration include: -

- Type of specialty the individual cited in the alert has previously targeted.
- Previous involvement with Mental Health Services.
- Previous attendance within the North West.
- Types of crime committed.
- Specific directions by the SMS as included in the alert.

6.31 If the decision is to forward the alert to staff within the Trust, a log is made of who it is sent to, when and if specific directions are requested. If it is not appropriate to send the alert to the Trust Staff, the reasons for this decision are logged.

6.32 Making a referral to the SMS for an Alert to be made

6.33 On occasion it will be appropriate to request that the SMS share an alert about one of the trusts service users behaviour and risks to staff in other trusts. This will usually be when a service user is missing, but could also relate to specific behaviours the person may display on a regular basis and the concerns that other local trust staff are at risk. .

6.34 The request should emanate from Clinical staff who will discuss their concerns with the LSMS who will consider the validity of making such a requests, the decision made will take into account-:

- Validity of breaching confidentiality, in relation to the reduction of risks and prevention of a crime -individual legal advice can be sought to ensure confidentiality is not inappropriately broken.

- The need to seek permission from relatives/ carers in relation to sharing personal information of a service user.

- The level of risk the individual poses to the staff who work in other trusts

- Recommendations from other external staff including, police and probation services.

6.35 If it is agreed to refer to the SMS, the LSMS will complete the referral form, and share with the Regional SMS manager. The reasons for the actions taken will be documented within the service user's clinical records. The use of the alert system will also be logged on the Trust alert data base.

6.36 Multi Agency Public Protection Arrangements (MAPPA) / Health Risk Assessment and Management Meetings (H-RAMM)

6.37 The Trust is actively engaged with the use of Multi Agency Public Protection Arrangements **(**MAPPA**) /** Health Risk Assessment and Management Meetings (H-RAMM). These systems are used to facilitate the joint working of different agencies include the Police, Probation, Housing and Health in order to co-ordinate the management of high risk individuals.

6.38 The Criminal Justice Liaison Team co-ordinate the Trust's involvement with MAPPA panels: -

- Triage referrals for MAPPA meetings.
- Chair and co-ordinate the H-RAMM meetings.
- Record and monitor MAPPA usage within the Trust.
- Develop and oversee implement of MAPPA / H-RAMM Policy and Procedure.

6.39 Managing Access and Egress

6.40 All sites should be secured and have the minimal number of entrances in operation. The preferred option is that: -

- Each unit has one entrance to the site, which provides a reception process.
- All corridor doors providing exit should be secured in accordance with Fire Safety Policy.
- All departments contained within a unit / site should have their entrance and exit secured.

6.41 The primary focus for security is always targeted at ward / department level with the unit entrance and associated security providing a secondary level of security.

6.42 Reception Process

6.43 <u>Generic Information</u>

- Each unit / site (clinical and non clinical) should have an ability to receive people entering the building with the aim of directing them safely to their destination and clarify any safety regulations with them.
- Each visitor to a unit should sign in at Reception – using the agreed Trust wide system.
- Each visitor (not receiving clinical services) should be issued with a visitor's badge.
- Each NHS employee should display their badge at reception and sign the Fire register.
- All visitors should sign out of the building and return the visitor's badge to reception.
- Within clinical areas / departments, a register of service users who are on the ward at any given

time should be kept in accordance with Fire Safety procedures.
- All people entering the ward / department must be greeted and directed to where they need to go.

6.44 In-patient Areas

6.45 Inpatient Services are continuously involved in securing the entrance to all wards (This procedure does not direct practices within High, Medium or Low Secure Services which are governed by specific security procedures).

6.46 This involves: -

- Continuous locking of the external ward door using digital fob-activated systems that have been fitted to all areas.
- Staff taking responsibility for letting people in and out of the ward. (The doors are locked 24 hours a day throughout the period when this level of safety and security is in place).
- Where used, digital codes are held confidentially and changed on a regular basis.

6.47 Rationale

6.48 The decision has been made to enhance the safety of vulnerable adults who are cared for within the inpatient areas by ensuring that individuals do not leave the ward without prior agreement. This system will also allow staff to monitor who enters the ward area and potentially reduce the ability for people to bring inappropriate items into the ward e.g. drugs, alcohol etc.

6.49 It is not envisaged that these arrangements will unduly affect the ability of individuals who are able to leave the ward to do so. These arrangements should ensure that those leaving are seen by staff before exiting and times of return agreed and documented. A risk assessment should take place which identifies the suitability of each service user to take leave from the ward.

6.50 It is essential that each ward adopt a reception process that will allow people to be greeted onto the ward and directed appropriately.

6.51 Ward Based Reception

- At all times there will be a member of staff allocated to fulfil the reception function and this individual is expected to coordinate access and egress to the ward. In the main they will be carrying out decisions agreed by the Multi-Disciplinary Team regarding the suitability of people to enter and/or leave the ward. Any

requested digression from the agreed care plan must be discussed with the nurse in charge first and documented.

- If any staff on reception duty are concerned about the appropriateness of anyone leaving or entering the ward they must seek clarification from the nurse in charge prior to taking action e.g. a service user may suddenly become distressed or a visitor is suspected of being intoxicated.

- The member of staff allocated this role will have an up-to-date list of service users who are able to leave the ward. This list will be continuously updated at the start of every shift and at other appropriate times –i.e. after a ward round.

- It is **essential** that service users who are not detained under the Mental Health Act (2007) are not prevented from leaving the ward inappropriately by the door being secured. If staff are concerned about the mental health of an informal service user who wishes to leave the ward, a mental health assessment must be facilitated immediately and use of the MHA (2007) considered.

- Any delays in allowing service users to leave the ward should be recorded in their clinical records, with appropriate reasons.

- Staff who fulfil this role will at all times be polite and professional in their manner. This role does NOT require the nurse to sit at the door; this way of working is actively discouraged. The reception role should allow staff to continue with other tasks/work as long as they are able to respond to a request to enter or leave the ward within an acceptable time period (max 5 minutes).

6.52 The staff on reception duty will undertake the following: -

Access	Egress
• Open the door to let people enter the ward • Ensure that it is appropriate for the individual to enter the ward by: o Wearing of visitors badge, staff identity badge o Suitability of the environment to accommodate visitors at that time	• Document when a service user leaves the ward and when they are due to return. • Provide information to service users as to why they cannot leave, and direct them to other staff who can talk to them about their

o Consult list of people that the Multi-Disciplinary Team do not wish to enter the ward • Welcome people to the ward. • Direct visitors to the individual they have come to see • Provide advice and guidance regarding accepted behaviour on the ward. • Prevent people entering the ward if service users do not want to see certain individuals • Prevent individuals entering the ward if it is felt that they are bringing in unacceptable items i.e. drugs and or alcohol.	concerns in more detail. • Ensure that people do not congregate at the door, as this will create difficulties in the case of an emergency. • If staff feel threatened and in danger, because they are not allowing a person to leave the ward, they should immediately call for help using the alarm system. • If extra staff cannot calm the situation, the following should be considered: - o Mental Health Act Assessment for non detained service user. o Emergency use of Section 5/4 MHA 1983. o Emergency call to the Police, requesting their attendance to subdue a dangerous situation. o Letting the person leave and implement the Service users missing from an inpatient area Policy (SD05). o Use of lockdown Procedure if risk assessment advises that the person would be a danger to themselves or others, if released and immediate action is required. o Use of Control and Restraint Procedure.

6.53 Door Management

➢ **Non Clinical Areas**

6.54 Staff allowing people to enter a building should: -

- Ensure the person can provide proof of identity and a valid reason for being on the premises.
- Direct the individual to their point of contact.
- Refuse entry if they are unsure of who the person is or why they need to enter the building.

6.55 Staff must ensure that doors are closed behind them.

➢ **In-patient Units**

6.56 Doors have been secured to ensure that staff can assess service users prior to them leaving the area. Therefore it is essential that the entrance door remains secured at all times and is only opened by authorised staff. Each Modern Matron has the responsibility of agreeing with the LSMS which members of staff will be allowed to have access to a key/fob/ security code. The allocation of keys to temporary staff, non clinical staff and visiting staff should only be undertaken if their access to the wards is seen as essential and not having a key would negatively affect the management of the ward.

6.57 Each key holder must: -

- Attend Key Access training prior to being given a key.
- Understand that breach of procedures will lead to permanent or temporary removal of key (Modern Matron and LSMS will make the decision).
- Carry fob/key securely on their person at all times
- Not give fob/key to any other member of staff(unless in an emergency)
- Not share door code with any other member of staff unless in an emergency
- Understand that clinical staff should only allow service users out of the ward who have been risk assessed as being suitable by clinical staff.
- Ensure that Non Clinical staff should not open the door to allow service users to leave the ward.
- Ensure that the door area must not be used as areas for discussion and informal gatherings.
- Understand that the person opening the door is responsible for ensuring it is shut behind them.
- Accept that the person opening the door to visitors is responsible for asking the person their names and directing them to the nurse responsible for access and egress during the shift.
- Identify any person who wishes to leave, before they open the door and confirm they are able to do so thus preventing tailgating.
- Understand that non clinical staff are only able to use key fobs to let themselves in and out of wards.

6.58 Tail - Gating

6.59 Tail-gating in relation to security, is the practice of a person entering or leaving a premise whilst another person has opened the door. The

person will normally follow the person out openly or go through an unsecured door after the key operator has left the scene. It is important to note that the person, who is opening the door, has responsibility for: -

- Ensuring it is closed behind them.
- Ensuring that anyone exiting / entering with them is able to do so.

6.60 Anyone trying to enter or leave inappropriately should be asked to wait and clinical advice sought.

6.61 Search Process

6.62 Staff can request permission to search visitors to the ward, if they have evidence that inappropriate items are being brought onto the ward. This must be undertaken in accordance with the Trust's Policy and Procedure for the Searching of service users, their Room Possessions, Lockers, Personal Property and Ward Area (Local Services) – *SD20* and with due consideration of privacy and confidentiality.

6.63 Generally this will mean that staff will search a visitor's bag or outer clothing, if further searches are required, consideration should be given for not allowing the person to enter the Unit.

6.64 Carers / Service Users ability to Access Wards

- It is essential that on admission each service user and their carer receive information regarding the security measures the Trust has adopted this should be done orally and in writing.
- Each ward must display clear information near the exit, stating how service users/carers can access help to leave the wards i.e. who they need to ask.
- Staff who are responsible for reception duty should be clearly visible and able to assist service users/carers with the shortest possible timescale.
- A notice will be situated just outside the door informing people of how they may gain access, which will include the maximum time they could expect to wait for a response.
- The information provided to service users and carers must include any criteria used to make decisions re a person's suitability to enter i.e. wearing identity badges. This should also include any behaviour which will prevent access the ward i.e. being verbally abusive.
- The unit reception staff will be provided with a list from each ward (on a daily basis) of

individuals who do not have access to the wards. If these people try and enter the unit, they should be asked to wait whilst a member of the ward staff comes to explain why they are not being allowed entrance. Where possible this should be done in a quiet area of the unit. The only exception to this will be if there is an identified level of risk then the reception area can be used.

- If service users have stated that they do not wish visits from certain people, then the service user or staff member should immediately inform the person via the telephone.
- Allowing children on the ward will be undertaken in line with the Child Visiting Policy. (**SD22:** Children visiting Mersey Care sites)

6.65 At no time will staff be expected to put themselves or others at risk while carrying out these duties.

6.66 Lockdown Guidance

6.67 The definition of lockdown is as follows:

'lockdown is the process of preventing entry, exit and movement around a Trust site or other specific Trust building/area, in response to an identified risk, threat or hazard that might act upon the security of patients, staff and assets or indeed the capacity of that facility to continue to operate'.

6.68 The purpose of a lockdown is to confine the aggressor to a certain area allowing enough time for assistance to arrive and take control of the situation. In addition it can be used to allow a physical barrier to separate the aggressor and staff reducing the risk of demonstrable violence.

6.69 Within this organisation the main uses of lockdown would be: -

- To isolate an affected area or a violent individual for a short time until help from the Police arrived.

- To lockdown a Unit to prevent contamination from external major incidents or during terrorist alerts.

6.70 Examples of Incidents which may lead to lockdown

Incident	Action	Lockdown
Suspicious package	Isolate and call police	Advised safe: No Advised possible IED: Yes
Violence & Aggression	Control locally and call the police for help if required	No
Violence and Aggression using a weapon and holding hostages	Call the police	Local lockdown
Fire	Call the emergency services Evacuate buildings following action plan	Progressive lockdown following directions from the fire service
Terrorist on site	Call police	Yes
Chemical / biological contamination	Call emergency services	Yes

6.71 Local Protocols

6.72 Each service must have a 'Lockdown Protocol' – this policy will identify key points that should be included in local documents.

6.73 Throughout the lockdown and before agreeing to a lockdown the Nurse in Charge / departmental manager must, ensure that: -

1. Staff understand the actions they must take.
2. Agree how communication with any service users, who are isolated, will be maintained.
3. Balance the risks between isolating the service user and organising physical intervention (Personal Safety Training)
4. Ensure observation is maintained of the area and where possible the isolated service user
5. Where the service user is isolated, staff must review the efficacy of continuing with a lockdown, every 15 minutes and document the decisions made.
6. Where buildings are closed down, the timescales can be agreed locally but should be reviewed hourly.
7. Ensure all affected staff and service users understand what is happening and when the lockdown is likely to end.

6.74 Tasks undertaken should be completed without placing staff at unnecessary risk. These include: -

- The locking of doors/windows
- Contacting security staff for assistance (if possible)
- Contact Police (if necessary)
- Provide security staff/Police with as much information as possible prior to intervention
- Refraining non essential staff and patients from entering the area
- Placing staff at entry points to stop others from entering the area
- Ensure CCTV, if fitted, remains 'on' (visual or audio) if applicable
- Inform Bronze on Call that a lockdown is occurring and document it as an Adverse Incident.
- Review and assess situation following incident

6.75 Local Protocols should be written taking into account the layout of local buildings, staffing levels and how to access assistance. All risks should be identified and management regimes clearly outlined. The aim of any lockdown procedure is to: -

- Maintain the safety of staff, service users /carers
- Minimise the amount of harm that can be caused by violent and dangerous behaviour
- Maintain safety until sufficient staff and/or external help can be obtained to manage the situation effectively
- Prevent contamination from external sources and maintain the ability of the organisation to keep staff and service users safe.

6.76 This guidance regarding a lockdown procedure is not intended to cover every situation and the staff member in charge of managing the incident and lockdown should assess the individual circumstances on a 'case by case' basis and respond accordingly involving the support available in the Trust and from external agencies.

6.77 Development of Local Lockdown Protocols

6.78 The LSMS will be accountable for ensuring that the Local and Secure Clinical Divisions/Corporate Division[1] have a portfolio of Lockdown Procedures in place. They will work closely with each of the Risk Management Leads in each CBU/corporate service to provide guidance

[1] (where relevant i.e. in the event of a major incident)

regarding the content of each Lockdown Protocol. Each Risk /Security Lead will develop the Lockdown Protocol and once agreed with the LSMS, it will be taken to the local governance forum for ratification.

6.79 The annual security report will include a section on the availability of Lockdown Protocols in each CBU/corporate area, usage and risk identified. This process will be used to monitor adherence to this important part of the policy and direct actions to be taken to eradicate any deficits identified (See Appendix 6 - Flow Diagram).

7 CONSULTATION

7.1 This Policy has been developed as a result of the evaluation that took place in clinical services regarding the use of locking mechanisms which identify a lack of a clear understanding by staff of Security and how to monitor it. When implemented, the policy will support the aim of balancing safety and confinement in a way that is supporting an approach that is sensitive to the rights, needs and views service users. Consultation has taken place with: -

- Head of Quality & Risk
- Modern Matrons
- Ward Based Staff
- Local Division risk manager (Liverpool)
- Risk Manager
- Governance Forums within the Divisions

8 TRAINING AND SUPPORT

8.1 All clinical staff receive Security and Fraud awareness training as part of mandatory training in the prevention and management of violence by the Personal Safety Service (see policy SD18)

8.2 Staff familiarisation with this policy and local security arrangements for building (including lockdown) should be incorporated within local induction

9 MONITORING

9.1 Monitoring of Security Activity

9.2 The Quality Assurance Committee will receive an annual report which will contain: -

9.3 Trends analysis of security incidents including physical assaults and breaches to building security.

9.4 Identification of continuing security risks.

9.5 Summary of findings from annual and three yearly security audits.

9.6 Outline adherence to this policy, citing areas where improvement is required and when and how this will take place.

9.7 The work-plan of each LSMS will be agreed annually with the Security Management Director and Security Management Service reflecting the findings of the above and will be targeted at improving prioritised risk areas

9.8 A Security Monitoring Group will be in place to: -

- Advance security practice across the Trust
- Review trends in relation to security incidents
- Prescribe remedial action
- Report to the Health & Safety Committee

9.9 This group will have representation from each of the service specialties. The individuals attending will be those having a role in managing security. The group will meet on a quarterly basis and be chaired by a LSMS.

10 Appendix 1

Security Risk Assessment

10.1 This Security Risk Assessment is to be completed by the Premises Manager on an annual basis as a minimum or more frequently if required. If guidance, advice or assistance is required to complete certain sections of this risk assessment, the LSMS shall meet this request.

10.2 The LSMS shall contact each Premises Manager and ask for a copy of the completed Security Risk Assessment to be sent to the Risk Management Department on an annual basis for auditing purposes and to ensure that this policy is implemented.

Mersey Care NHS
NHS Trust

APPENDIX 1

SECURITY ASSESSMENT

Building: **Date of Assessment:**

Overview of Service:
(age of building, number of people using building, type of client, number of exits, previous incidents)

Action Key: 1 Local Manager to action
2. Service Manager to action
3. Entry onto Local Division Risk Register

Red = High **Amber = Moderate** **Green = Low**

THERE ARE ADEQUATE PROCESSES FOR CONTROLLED ACCESS/ EGRESS

	Yes	No	N/A	Key	Risk	Action needed:
▪ Are there posters and information clearly in place - advising how to obtain entry and exit?						
▪ Is there a keypad system/digilock in use to control access and egress?						
▪ Is there an intercom system in place?						
▪ Is there a signing in book procedure in place?						
▪ Are Visitor's badges given to non-Trust staff?						
▪ Is there a reception process in place to control who enters the building?						
▪ Are visitors encouraged to use the main door and is this clearly signposted?						

	Yes	No	N/A	Key	Risk	Action needed:
▪ Are visitors asked to sign in and out?						
▪ Are visitors escorted to their destination?						
▪ Are members of the public prevented from entering unauthorised areas of the buildings?						
▪ Do staff challenge strangers whom they see in the building?						
▪ Is this process adequate? *What hours does is cover (i.e. 24 hours, 9-5)?*						

KEY AND LOCKING UP

	Yes	No	N/A	Key	Risk	Action needed:
▪ Is there a proper system to control the issue of keys?						
▪ Is there an established procedure for locking up?						
▪ Are persons who use the building outside normal hours briefed on securing the premises when they leave?						
▪ Is there a procedure for periodically checking security fitting such as locks, catches and bolts?						

SECURITY OF BUILDINGS

	Yes	No	N/A	Key	Risk	Action needed:
▪ Are the premises in good repair?						
▪ Has consideration been given to protecting or eliminating recessed doorways, concealed yards, shrubs, planted areas and similar features which can give cover to intruders?						
▪ Is the main building free from examples of flimsy structures such as low-level glazing or lightweight panelling?						
▪ Are all entrance doors locked and windows and skylights secured when the premises are not in use?						
▪ Have steps been taken to restrict easy access to the roof from points such as lower, adjacent structures, compounds, walls, down pipes?						
▪ Are tools and ladders locked securely away?						

THE INTERNAL SECURITY OF BUILDING ACTS AS AN APPROPRIATE DETERRENT

	Yes	No	N/A	Key	Risk	Action needed:
▪ Is the reception area at a height to deter service user's jumping over?						
▪ Is there an adequate screen to protect staff from assault?						
▪ Does the reception staff have clear sight lines to identify which service users are coming into the building?						
▪ Do the reception staff have access to a panic alarm?						
▪ Do the reception staff know how to call and when to summon the police?						
▪ Is there controlled egress and access into the reception area?						
▪ Are staff offices and toilets locked with controlled egress and access?						
▪ Are drugs and cleaning agents locked securely away?						
▪ Is furniture fit for purpose and adequately secured to prevent barricades or assault?						
▪ Are doors designed to prevent absconsions?						

	Yes	No	N/A	Key	Risk	Action needed:
▪ Is there an adequate panic alarm in place?						
▪ Is a protocol in place that clearly states how staff respond to this alarm?						
▪ Are CCTV cameras in operation and recording activity?						
▪ Are there signs in place to advise service users of CCTV?						
▪ Are there adequate prosecution signs in place warning services users of action by Trust?						
▪ Is there a designated place to interview/de-escalate potentially disturbed/aggressive individuals?						
▪ Is there a designated Key Holder for the building and during which hours would they be expected to respond?						
▪ Is there a designated Site Manager /nominated lead for security issues?						
▪ Has the Crime Prevention Officer been involved in assessing the general security of the building?						
▪ If so, have the recommendations been actioned?						

	Yes	No	N/A	Key	Risk	Action needed:
▪ Is the MHA Tribunal Room fit for purpose (design, layout, panic alarm)?						
▪ How does the unit control prohibited items coming into the unit. Is this adequate?						
▪ Does the unit use passive/active search dogs?						
▪ Is there a working visible intruder alarm system and box in place on the building?						

THE EXTERNAL SECURITY OF THE BUILDING ACTS AS AN APPROPRIATE DETERRENT

	Yes	No	N/A	Key	Risk	Action needed:
▪ Is there CCTV coverage of the perimeter of the building?						
▪ Are all fire exits into the building secured appropriately?						
▪ Is there allocated parking areas for staff?						
▪ Do staff have access to personal attack/rape alarms outside the building?						
▪ Is there adequate outside lighting at night around parking areas?						
▪ Are staff advised not to leave personal						

	Yes	No	N/A	Key	Risk	Action needed:
belongings, mail and ID badges on display in their cars?						
▪ Is there clear access for emergency vehicles and personnel outside the building?						
▪ Can staff be escorted to their cars by security staff in the evening?						
▪ Are there any local community issues that impact on staff's safety?						

ALL STAFF ARE ADEQUATELY TRAINED IN PERSONAL SAFETY ISSUES

	Yes	No	N/A	Key	Risk	Action needed:
▪ Have all relevant staff attended the appropriate Trust MVA Breakaway Course?						
▪ Have all relevant staff attended the Trust Verbal De-escalation course?						
▪ Have all relevant staff attended the Trust 5 day Physical Intervention course?						
▪ Do all staff have access to an internal Personal Alarm System or how to summon help in an emergency?						
▪ Are staff aware of the Lone Working Policy? How is this evidenced?						

	Yes	No	N/A	Key	Risk	Action needed:
▪ Is there a monitoring system to ascertain the whereabouts of community staff at all times.						
▪ Are staff aware of the Search Policy and know when to use it appropriately? How is this evidenced?						

CONTRACTORS

	Yes	No	N/A	Key	Risk	Action needed:
▪ Is a named person designated to ensure that statutory controls are properly applied and that the appropriate extra security, safety and fire precautions are taken when contractors are working on the premises?						
▪ Are pre-contract meetings held between interested parties to identify on-site risks and procedures necessary during the work, including the raising of security?						

ATTRACTIVE TARGETS

	Yes	No	N/A	Key	Risk	Action needed:
▪ Have special arrangements been made to protect items of particular interest to thieves, such as food stocks, tools, solvents and drugs?						

LOCKDOWN

	Yes	No	N/A	Key	Risk	Action needed:
▪ Are there means to 'lockdown' vulnerable area of the premises if necessary?						
▪ Are there means to raise the alarm?						
▪ Can security personnel / emergency services be swiftly contacted for assistance?						
▪ Are staff aware of the 'lockdown' guidance section within the Security Policy?						
▪ Has the need for a lockdown procedure been identified by the Premises Manager?						
▪ Has this procedure been written and issued to relevant staff?						
▪ Are there means to monitor the individual within the holding area without placing yourself at risk?						
▪ Is there a need to contact the LSMS for further advice to the level of risk?						

ALL STAFF ARE FULLY SUPPORTED FOLLOWING AN INCIDENT AND AWARE OF SUPPORT SYSTEMS AVAILABLE TO THEM

	Yes	No	N/A	Key	Risk	Action needed:
▪ Do staff have input into a police liaison meeting?						
▪ Are staff aware of how to access staff services?						
▪ Are letters of support sent to staff by the local manager following an incident?						
▪ Do post incident discussions take place and are they documented appropriately?						

Name of person completing assessment:

Is further assessment necessary? **Yes/No**

Review Date:

Additional Comments:

Appendix 2

Mersey Care NHS Trust

Security Assessment Following a Breach

Site ……

Assessed by……

Requested by ……..

……

Reason for Assessment (Incident – type, date, time)

……...

……

Key Findings – External ……

……

……

Key Recommendations – External ……

……

……

Key Findings – Ground ……...

……

……

Key Recommendations – Ground ……

……...

……

Key Findings – 1st Floor ……

……

……

Key Recommendations – 1st Floor ……

……

……

Key Findings – 2nd Floor ……

……

……

Key Recommendations – 2nd Floor ……

……

……

Likelihood of re-occurrence ……

……

……

Overall Recommendations ……

……

……

Actions to be taken and by whom
(Actions should be written in prioritised order)……...
Action Key: 1 Local Manager to action
2. Service Manager to action
3. Entry onto AMH Risk Register

……..

……

Risk Rating

Red = High **Amber = Moderate** **Green = Low**

……

……

Assessment carried out by LSMS

Name ……..……..

Date ……../……../……

Appendix 3

The Ten Principles of Crime Prevention

The Home Office has produced a guide to crime prevention which may assist when looking at building security risk assessments.

1. Target Hardening
2. Target Removal
3. Remove the Means to Commit Crime
4. Reduce the Payoff
5. Access Control
6. Visibility/Surveillance
7. Environmental Design
8. Rule Setting
9. Increase the Chance of Being Caught
10. Deflecting Offenders

1) Target Hardening

Target hardening means: “Making targets more resistant to attack or more difficult to remove or damage”. A **target** is anything that an offender would want to steal or damage. It could be an object, property, person or in some cases an animal, such as a valuable pet. Here are some examples of Target Hardening.

- Fitting better doors, windows or shutters
- Window or door locks
- Alarms
- Screens in banks and building societies
- Fencing systems
- Repairing damaged and derelict property.

2) Target Removal

Target Removal is: “Permanent or temporary removal of vulnerable persons or property” Quite simply this means making sure that any object in which a potential offender might be interested is not visible. This can include: -

- Removing radios from parked cars
- Placing valuable items in a secure location
- Demolishing derelict property
- Removing jewellery from shop windows at night
- Moving small vulnerable items nearer to cash tills in shops

3) Remove the Means to Commit Crime

The previous techniques are aimed at reducing the risks directly associated with the target. Removing the Means to Commit Crime looks at the problem from a different point of view. Removing the Means to Commit Crime means: “Making sure that material capable of being used to help an offender commit a crime is not accessible”. Examples of removing the means to commit crime are: -

- Locking up tools and gardening equipment
- Securing building materials such as scaffolding

- Removing bins away from windows or vulnerable roofs and locking them away

4) Reduce the Payoff

Reduce the Payoff means: “Reducing the gain for the criminal if a crime is committed” Examples of this include: -

- Using a safe to reduce the amount of cash held in a till
- Property marking to make items identifiable and therefore less valuable to the criminal.

5) Access Control

Access Control means: “Restricting access to sites, buildings or parts of sites and buildings.” There are many forms of Access Control. Some of them are quite complex, but some are relatively simple. They include: -

- Door locks (and making sure doors are shut)
- Identity cards
- Entry card systems
- Entry phones
- Separate entries and exits
- Combination locks.

6) Visibility / Surveillance

This principle is defined as: “Making sure that offenders would be visible if they carried out a crime.” Unlike any of the other principles, there are three types of surveillance, these are: -

- **Natural**
- **Formal**
- **Informal.**

Like all the other principles there is a range of methods and techniques that can be applied.

Natural surveillance - Involves modifying the exiting surroundings to increase visibility. It can include: -

- Pruning or removing shrubbery
- Improving or installing lighting
- Changing the height of fences

Formal surveillance - Uses technology or specialist staff who are employed or tasked to deter and identify actual or potential offenders.

It can include: -

- Deploying police and security staff store detectives
- Alarm systems
- Caretakers tasked with a security role
- Closed circuit television (CCTV) systems.

Informal or employee surveillance - This involves residents, employees and the community being encouraged to be vigilant and knowing what to do when they see a potential risk.

For example: -

Receptionists, office staff and local neighbours can be asked to spot potential problems. Procedures should be put in place to tell individuals or staff what to do if they see anything suspicious.

7) Environmental Design

Crime prevention using Environmental Design is a large topic.

It Involves: “Changing the environment of a building, a site, an estate or a town to reduce opportunities for committing crime.” The emphasis is on putting a range of preventive measures in place at the planning stage. Crime Prevention through Environmental Design (CPTED) can be used in exiting environments, or in new developments. It can include a whole range of features, such as: -

- Visibility/Surveillance
- Target Hardening
- Street and pathway layout
- Lighting.

8) Rule Setting

Rule Setting means: “The introduction of legislation, by-laws and codes of conduct, which set out what is acceptable behaviour.” There are many types of Rule Setting, here a just a few: -

- Wearing ID badges.
- Internal rules within businesses.
- Local by-laws, such as those limiting consumption of alcohol in public places.
- Signs prohibiting access to buildings or certain areas in buildings.
- Requests to report to reception.

9) Increase the Chance of Being Caught

“Anything that slows down an offender or increases their risk of being caught.” Preventive methods are more effective if the offender risks being caught. Anything that slows down an offender or increases the chance of detection is an effective method of prevention. This means that good Target Hardening increases the time it takes to enter a building and increases the chances of being spotted. The longer it takes to commit an offence, the more vulnerable the offender feels. Increasing the chance of an offender being caught can be achieved by: -

- Proper management of CCTV systems

- Lighting that makes offenders more visible
- Making sure security equipment works properly
- Putting several preventive methods in place, which slows an offender down even further
- Alerting offenders to the fact that CCTV systems and alarms are being used
- Publicising successes in detecting offenders.

10) Deflecting Offenders

This is the final principle of crime prevention and means:

“Diverting the offenders and potential offenders from committing crime.” This involves agencies working with young people and offenders to influence standards, thinking and attitudes. The aim is to prevent potential offenders turning to crime. Examples include: -

- Education programmes & schools programmes
- Drug action teams
- Youth groups and organisations
- Providing training and work experience.

This method of preventing crime is increasing and the introduction of Crime and Disorder Reduction Partnerships has encouraged multi-agency working.

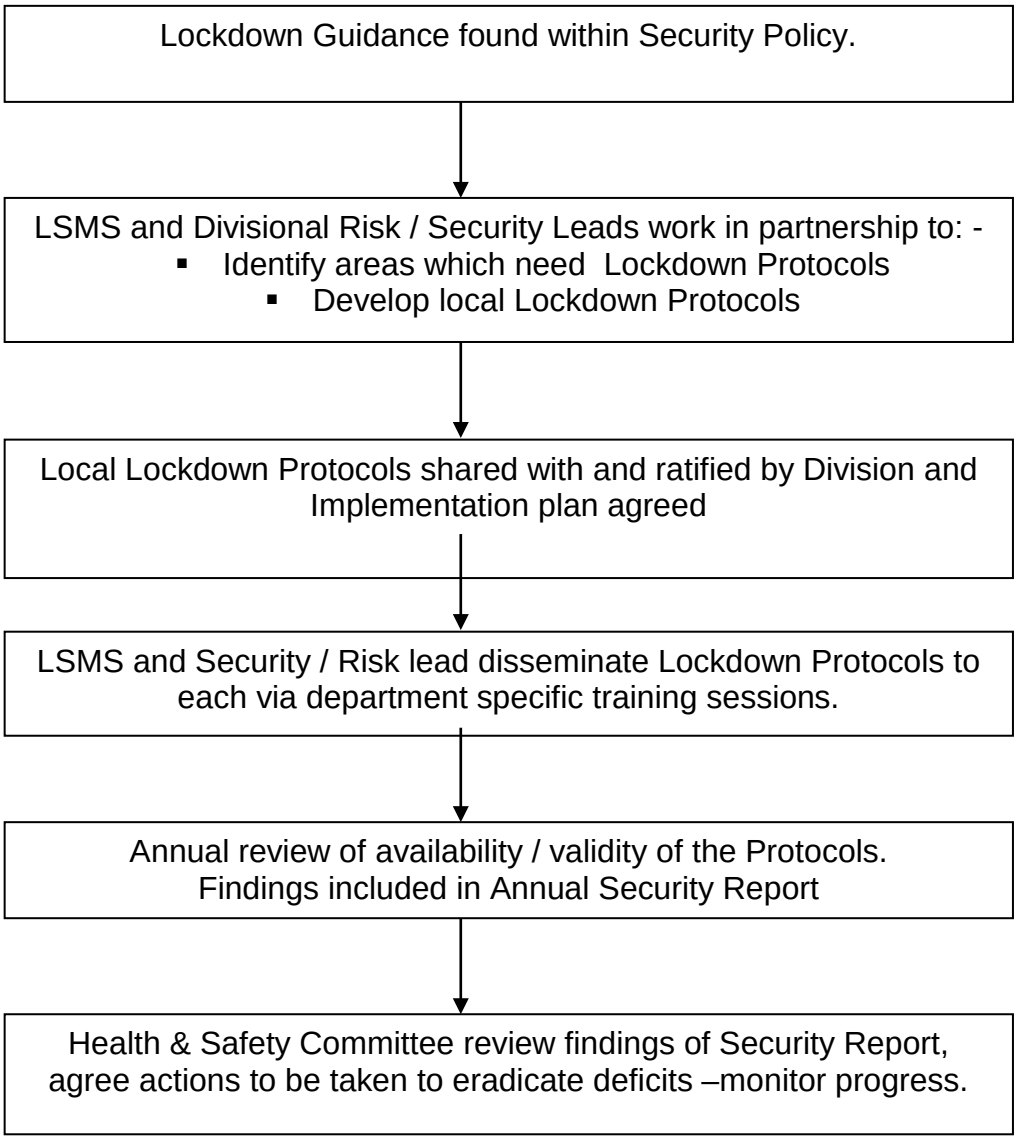
Appendix: 4

Glossary

- **LSMS:** Local Security Management Specialist
- **SMD:** Security Management Director in this Trust the role is undertaken by the Executive Director of Nursing and Care.
- **Tailgating:** When an individual follows another person through a door they have opened.
- **Lockdown:** Isolating an area or building to enhance the safe management of a building/incident.

Appendix 5

Development of Lockdown Protocols



Equality and Human Rights Analysis

Title:	**POLICY & PROCEDURE FOR THE MANAGEMENT OF SECURITY SYSTEMS (SA29)**
Area covered: Security	

What are the intended outcomes of this work? *Include outline of objectives and function aims*

the aims and objectives are;

(a) to ensure the security and safety of staff and visitors

(b) to ensure that Trust assets are managed effectively

Who will be affected? *e.g. staff, patients, service users etc.*

Applies to all trust staff and individuals visiting or using trust premises.

Evidence

What evidence have you considered?

Equality Information as published on the website in relation to the content of this policy

Disability (including learning disability)

No significant issues

Sex

No significant issues

Race *Consider and detail (including the source of any evidence) on difference ethnic groups, nationalities, Roma gypsies, Irish travellers, language barriers.*

No significant issues

Age *Consider and detail (including the source of any evidence) across age ranges on old and younger people. This can include safeguarding, consent and child welfare.*

Young persons at work –those under the age of 18years must be risk assessed prior to commencement of any work activities (i.e. nurse cadets, interns)

Gender reassignment (including transgender) *Consider and detail (including the source of any evidence) on transgender and transsexual people. This can include issues such as privacy of data and harassment.*

Sexual orientation *Consider and detail (including the source of any evidence) on heterosexual people as well as lesbian, gay and bi-sexual people.*

No significant issues

Religion or belief *Consider and detail (including the source of any evidence) on people with different religions, beliefs or no belief.*

No significant issues

Pregnancy and maternity *Consider and detail (including the source of any evidence) on working arrangements, part-time working, infant caring responsibilities.*

No significant issues
Carers *Consider and detail (including the source of any evidence) on part-time working, shift-patterns, general caring responsibilities.* No significant issues
Other identified groups *Consider and detail and include the source of any evidence on different socio-economic groups, area inequality, income, resident status (migrants) and other groups experiencing disadvantage and barriers to access.* No significant issues
Cross Cutting *implications to more than 1 protected characteristic* No significant issues

Human Rights	**Is there an impact?** **How this right could be protected?**
Right to life (Article 2)	*Use not engaged if Not applicable* Supportive of HRBA.
Right of freedom from inhuman and degrading treatment (Article 3)	*Use supportive of a HRBA if applicable* Supportive of HRBA.
Right to liberty (Article 5)	Supportive of HRBA.
Right to a fair trial (Article 6)	Supportive of HRBA.
Right to private and family life (Article 8)	Supportive of HRBA.
Right of freedom of religion or belief (Article 9)	Supportive of HRBA.
Right to freedom of expression **Note: this does not include insulting language such as racism (Article 10)**	Supportive of HRBA.
Right freedom from discrimination (Article 14)	Supportive of HRBA.

Engagement and Involvement *detail any engagement and involvement that was completed inputting this together.*

This was the annual policy review and other than being taken to the LSMS meeting & Health and Safety Committee there was no formal engagement

Summary of Analysis *This highlights specific areas which indicate whether the whole of the document supports the trust to meet general duties of the Equality Act 2010*

Eliminate discrimination, harassment and victimisation

Where appropriate the policy is supportive

Advance equality of opportunity

Where appropriate the policy is supportive

Promote good relations between groups

Where appropriate the policy is supportive

What is the overall impact?

The overall impact on the implementation on this policy review is minimal

Addressing the impact on equalities

There needs to be greater consideration re health inequalities and the impact of each individual development /change in relation to the protected characteristics and vulnerable groups

Action planning for improvement

Detail in the action plan below the challenges and opportunities you have identified. *Include here any or all of the following, based on your assessment*

- *Plans already under way or in development to address the **challenges** and **priorities** identified.*
- *Arrangements for continued engagement of stakeholders.*
- *Arrangements for continued monitoring and evaluating the policy for its impact on different groups as the policy is implemented (or pilot activity progresses)*
- *Arrangements for embedding findings of the assessment within the wider system, OGDs, other agencies, local service providers and regulatory bodies*
- *Arrangements for publishing the assessment and ensuring relevant colleagues are informed of the results*
- *Arrangements for making information accessible to staff, patients, service users and the public*
- *Arrangements to make sure the assessment contributes to reviews of DH strategic equality objectives.*

For the record

Name of persons who carried out this assessment:
Tony Crumpton: Head of Safety & Security
George Shield Senior Safety Advisor
Mark Clayton: Safety Advisor

Date assessment completed:
23/11/2015

Name of responsible Director:
Neil Smith – Executive Director of Finance (Deputy Chief Executive)
Deputy
Alison Jordan – Deputy director of Estates

Date assessment was signed:

Action plan template

This part of the template is to help you develop your action plan. You might want to change the categories in the first column to reflect the actions needed for your policy.

Category	Actions	Target date	Person responsible and their area of responsibility
Monitoring			
Engagement			
Increasing accessibility			