Mersey Care
NHS Foundation Trust

Community and Mental Health Services

TRUST-WIDE NON-CLINICAL POLICY DOCUMENT

Management of Security Systems

Policy Number:	**SA29**
Scope of this Document:	**All Staff**
Recommending Committee:	**Health and Safety Committee**
Approving Committee:	**Executive Committee**
Date Ratified:	**January 2020**
Next Review Date (by):	**January 2022**
Version Number:	**2020 – Version 5**
Lead Executive Director:	**Executive Director of Communications and Corporate Governance**
Lead Author(s):	**Head of Health Safety Fire and Security**

TRUST-WIDE NON-CLINICAL POLICY DOCUMENT

2020 – Version 5

Striving for perfect care and a just culture

TRUST-WIDE NON-CLINICAL POLICY DOCUMENT

MANAGEMENT OF SECURITY SYSTEMS

Document name	**MANAGEMENT OFSECURITY 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	**Carlton Brooks Head of Health Safety and Security** **Telephone: 0151 472 4071** **Carlton.brooks@merseycare.nhs.uk**
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** **Merseyside** **L34 1PJ** **Trust's Website www.merseycare.nhs.uk**
To be read in conjunction with	• SA18: CCTV Policy • SD3: Policy and Procedure for lone working • SD20: Policy and Procedure for the Searching of service users, their Room Possessions, Lockers, Personal Property and Ward Area (Local Services) • Lockdown Policy • SD32: Weapons in the Community Policy • IT02: IM&T Security • Security Directions for High Secure Services • SD37 Management of Service Users With Coexisting Problems Relating to Illicit Substances and Alcohol Use
This document can be made available in a range of alternative formats including various languages, large print and braille etc	
Copyright © Mersey Care NHS Trust, 2015. All Rights Reserved	

Version Control:

		Version History:
Stage of document, e.g., Consultation Draft, Version 1	Presented to the Executive and Health and Safety 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
Version 4	Policy re-write to reflect security management	18/12/2017
Version 5	Amendment to pages 1-3 and numbering	22 Jan 2020

SUPPORTING STATEMENTS

This document should be read in conjunction with the following statements:

SAFEGUARDING IS EVERYBODY'S BUSINESS

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

- being alert to the possibility of child / adult abuse and neglect through their observation of abuse, or by professional judgement made as a result of information gathered about the child / 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 / 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 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 Foundation 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 Foundation Trust recognises that some sections of society experience prejudice and discrimination. The Equality Act 2010 specifically recognises the *protected characteristics* of age, disability, sex, race, religion and belief (or lack thereof), sexual orientation, gender reassignment, pregnancy and maternity and marital and civil partnership status. The Equality Act also requires regard to socio-economic factors.

The trust is committed to promoting and advancing equality and removing and reducing discrimination and harassment and fostering good relations between people that hold a protected characteristic and those that do not 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 Foundation 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 Foundation 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

1.0 PURPOSE AND RATIONALE

NHS organisations are required to ensure that as far as is reasonably practicable that the delivery of healthcare takes place in a safe and secure environment. Healthcare settings are increasingly being seen by the criminal contingency of society as a soft target for both thefts and acts of vandalism. The difficulty has always been to balance the needs of visitors and service users for easy access against the legitimate protection of the Trust owned assets and the property belonging to both staff and service users. The Trust has developed this policy to help reduce such risks to a minimum.

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

The Trust will adopt a zero tolerance approach to thefts and acts of vandalism, It is important that all staff recognise and act on their responsibility in relation to security, *"keeping the NHS safe and secure is the responsibility of all who work in or use its services"* (NHS Protect, 2005).

2.0 OUTCOME FOCUSED AIMS AND OBJECTIVES

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, visitor's 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.

3.0 SCOPE

This policy applies to all Trust staff and individuals visiting or using its premises and relates to the security of persons, premises and assets. It includes the control of keys, fobs and access systems, CCTV, weapons in the community and liaison with the Police. All staff are expected to actively contribute to these security arrangements. 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.

4.0 DEFINITIONS

Physical security	This term relates to the security of premises, buildings, assets and objects (violence and aggression from patients/service users is detailed in the (Violence and Aggression Policy)
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.
Premises/buildings	The physical buildings in which NHS staff and professionals work, where service users are treated and from where the business of the NHS is delivered.
Assets	Irrespective of their value, assets can be defined as the materials and equipment used to deliver NHS healthcare. In respect of staff, professionals and service users it can also mean the personal possessions they retain whilst working in or providing services to the NHS.
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.
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.
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.
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.
Overt CCTV	This is CCTV monitoring which is not hidden, clearly visible and not intended or designed to monitor any specific activity or individuals. It is designed to allow the observation of an area for the recognition of any activity which may or may not occur. Overt CCTV is allowed without permission as long as certain rules concerning what is visible on the monitor are complied with.

5.0 ROLES AND RESPONSIBILITIES

5.1 Chief Executive

The Chief Executive has overall executive responsibility for security management within the Trust. This responsibility is delegated to Directors and Managers in the Trust.

5.2 Executive Director of Communications and Corporate Governance (Security Management Director)

This Security Management Director is responsible for ensuring that a strategic approach to improving the security within the organisation is taken. 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. The, Executive Director 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.
- 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.
- They are also accountable for ensuring the security issues are considered when new developments are being planned and developed within the organisation

5.3 Chief Operating Officer/Departmental Heads of Service

All Chief Operating Officers and Heads of Service are responsible for security for areas under their control. They are responsible for ensuring that staff are appropriately trained and that a security culture is embedded in day to day operations. They should ensure:-

- That the arrangements of this policy are communicated and adhered to by all staff under their control.
- That security risk assessments are in place for all areas under their control.
- 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
- Ensuring that the LSMS/ Divisional Risk Lead are 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.
- 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,

5.4 Head of Estates and Facilities

Duties of The Head of Estates and Facilities include:

- Ensuring appropriate physical security of Trust premises, including making arrangements for premises to be made secure as soon as practicable in the event of damage presenting a security risk.
- Ensuring the maintenance of security related systems such as alarm systems, access control and CCTV installations is carried out where the budget for these systems is held by Estates.

- Ensure that new builds and alteration work within the Trust includes funding for appropriate and agreed standardisation of physical security measures and products, which may include:

  - A means of access control whether it is keys, combination locks, fobs, and swipe card or proximity detectors.
  - An intruder alarm system
  - A CCTV system
  - External lighting to vulnerable areas.
  - Security measures to ground floor windows such as shutters, bars or grilles.
  - Staff attack systems

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.

5.5 Local Security Management Specialist (LSMS)/ Divisional Risk Lead

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

- A focus for security related matters.
- Receiving security related reports, including violence and aggression incidents and environmental incidents.
- Liaising with the police, including incidents where the police response has not matched expectations.
- Reporting all security incidents to the Head of Health Safety and Security including Divisional managers and following up all actions from any security incident. Publicising any security incidents, where lessons can be learnt.
- Provide an annual security report and Security Management Specialist annual work plan report for the Trust Board.
- Carry out security inspections of workplaces in conjunction with the service / area managers. Provide an action plan from that inspection and assist the manager to complete the actions identified.
- Conduct security surveys and security risk assessments where a workplace security inspection demonstrates a more detailed risk assessment is required.
- In conjunction with service managers create a lockdown risk profile for each property/site within the Trust.
- Assist in drawing up specifications for security improvement work identified through surveys in conjunction with the service managers.
- To carry out investigation following a security related incident and produce a report with recommendations for further action.
- Acting as an Authorising Officer for the release of CCTV and other images.
- The implementation and maintenance of a CCTV inventory by location, number of cameras, licences and authorised users registered for the purpose of data protection and image release.
- Approving the release of the material to authorised officers and keeping signed records of such releases in accordance with the Data Protection Policy.
- Obtain images/ video clips in connection with any security incident in compliance with the Data Protection Policy.

5.6 Divisional Risk / Security Leads

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.

5.7 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 manager/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.

5.8 Security Monitoring Group (SMG)

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 the Head of Health Safety and Security.

The SMG will be responsible for

- Reporting to the Health and Safety Committee
- Maintaining advance security practices across the Trust
- Reviewing trends in relation to security incidents
- Prescribing remedial action to address deficiencies in security management.
- Formulating and agreeing the annual security work-plan
- Ensuring that actions arising from the annual security work-plan are completed

5.9 Individual staff members

All staff employed within the Trust are responsible for:

- Complying with security procedures that are relevant to their respective work place.
- Making full use personal protection/alarm devices and of any installed security measures within their own building.
- Making full use of security devices which may be issued to them on an individual basis.
- Reporting suspicious activity or actual incidents on the incident reporting system.
- Reporting what they believe to be a serious security incident to the local Police, their manager and to the Trust's Safety Team.
- If safe to do so, politely requesting any unknown person within their area of work to reveal their identity and nature of their business.
- Failure of any person to give such details should be treated as a security incident and reported immediately.
- Wear their Trust ID badge at all times whilst on duty. If the visible wearing of a Trust ID Badge is not suitable, the member of staff MUST have the ID badge on their person and must produce it if requested.
- The reporting of any suspicious activity that they believe could lead to, or actually is, fraudulent, to the Counter Fraud Specialist.
- Within HSS staff will use the 5 x 5 security intelligence /incident reporting system is used.

5.10 Temporary or Agency Staff, Contractors, Students or Others

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.

6.0 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.

6.1 How the Trust risk assesses the physical security of premises and assets

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

6.2 Annual security risk assessments (See appendix 2)

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 program.
- Control and prevention of prohibited items entering the department i.e. alcohol and illicit substances, knives, lighters etc.

Divisional service leads with the LSMS/Divisional Security Lead will co-ordinate and facilitate the implementation of the assessments process.The inspection findings will be entered onto a divisional database in order to monitor that risk assessments are taking place and to inform the required organisational overview.

Control measures identified by the risk assessment shall be implemented by the service manager. If risks are not, or cannot be managed at a local level, they will be escalated by the manager through the risk register process.

Risk assessments will be reviewed every two years or sooner where circumstances dictate e.g. security incidents, change of building function etc.

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

6.3 Assessment following a security breach

All staff have a duty to report a crime. Once a crime has been reported, the LSMS/ Divisional Security Lead 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.

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.

6.4 Arrangements for the organisational overview of risk assessments of the physical security of premises and assets

- The Safety Team will maintain and monitor a database of security risk assessments provided by managers regarding the physical security of premises and assets.
- The Health and Safety Committee will monitor completion of risk assessments through the Quality Reporting in order that an organisational overview is maintained.
- Where gaps are identified this will be notified to the relevant manager with timescales for completion and submission of the risk assessment.
- In multi-occupancy buildings, the managers of the various services within the building must liaise and agree a process for the completion of the Security Risk Assessment and management of security in general.
- The Safety Team will provide assistance to the manager if required. If an area has complex security needs, the Safety Team will work with the manager to complete a more detailed risk assessment. All issues identified in the risk assessment which require control measures are to be included in an action plan.

6.5 How action plans are developed as a result of risk assessments

Recommendations made from risk assessments will be collated into an action plan. The issue will be discussed with the manager and the required action implemented via the appropriate service for example the Estates Department.

The action plan and implementation will be agreed by the divisional sub safety committee/group and will contain the following:-

- Who has overall responsibility for the action plan (if not the manager)
- What the risk is
- What is required to mitigate the risk
- Who is responsible for the required action
- When the action is to be completed

The manager is to forward a copy of the action plan to the Safety Team with the risk assessment.

How action plans are followed up

- The completion of an action plan is the responsibility of the Manager of the area it applies to.
- The LSMS/Divisional Security Risk Lead (and/or Safety Team) will provide assistance to the manager if required.
- An update on the action plan will be requested near the completion date, and an exception report will be presented to the Estate Management Team where the risk is deemed high or significant.

A corporate action plan will be developed and managed by the LSMS/Divisional Risk Lead 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.

6.6 Capital Projects

When a new building is being developed or an exiting building is being re-modeled, the LSMS/ Divisional Security Risk Lead 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.

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.

6.7 Premises Security Contracts

An external security provider is contracted to deliver specific security management services within Trust buildings. The LSMS/Divisional Security Risk Lead will ensure that the following is applied to each Trust owned/managed building:

- That a database of all Trust property is maintained and shared with the contractor.
- That all acquired or new buildings are listed on a database.
- That each building has a security assignment instruction that covers opening/closing of buildings, responding to security alarms, break-ins and CCTV maintenance.
- That the security provider is provided with keys/fobs and access codes of each building.
- That the security contract is reviewed annually with the contractor.

6.8 Security of Trust Buildings and Assets

The below list relates to properties and assets which are in the managed by or are in the control of the Trust:

- All buildings will be provided with a means of access control whether it is keys, combination locks, fobs, swipe card or proximity detectors. If the building has a public access area such as a foyer or corridor, then access control should ensure that non-public areas are secure.
- All buildings where appropriate will be provided with an intruder alarm system appropriate.
- Vulnerable external areas of properties will be provided with external lighting.
- All buildings / departments must have a named person who is responsible for coordinating the security of the area i.e. Site Manager.
- All buildings are to be left locked and secure, with appropriate security systems activated, access doors and gates locked and keys returned to relevant key holding areas.
- Within HSS MSU and LSU workmen and contractors are escorted.
- All thefts / burglaries to property should be reported via the Adverse Incident Process so that the incident is logged and trends monitored.

- All staff are to be aware of the security of the building and their role in maintaining the security. This includes familiarisation with the lockdown process.
- Buildings which are not managed / occupied over 24 hours should be alarmed and linked to a contracted security provider.
- All staff are to be aware of the security of the building and their role in maintaining the security. This includes familiarisation with the lockdown process.
- 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
- 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.

Where properties and assets are shared/ not under the direct control of the Trust:

- Trust staff are to assist the property owners/managers and other occupants to maintain security of the property and its assets.
- If the building does not meet the requirements of this policy, the relevant Manager will discuss the matter with the building owners/managers and come to an agreement on how to ensure the building security is adequate to protect Trust staff and property. If an agreement is not possible, the matter is to be reported to the Safety Team.

6.9 Personal Security of Staff

The Trust has taken a number of measures to protect the personal security of its staff which includes:

- The installation of security and panic attack alarms systems where a need has been identified.
- Issue of lone worker alarm devices where identified by risk assessment.
- Installation of staff attack alarms and systems throughout inpatient areas.
- Provision of suitable training for staff.
- The adoption of a zero tolerance approach in relation to acts of theft, vandalism or assault.
- Use of CCTV in areas that have been identified by risk assessment.

Where possible the Trust will aim to standardise Staff Attack Systems (SAS) and CCTV provision across all sites to aid staff familiarity with installed physical security measures.

6.10 Weapons in The Community

The use of and access to weapons by individuals in society is recognised nationally as being problematic. There have been high profile incidents that have involved individuals who have had a diagnosed mental illness, either injuring people with a weapon or being injured because they did or were thought to have a weapon.

It is recognised that any object involved in threat or attack can be described as a weapon and commonly include knives, broken glass, needles and other sharp objects. Also seemingly innocent household items could easily be utilised to threaten or cause injury e.g. Cutlery, baseball bat, chair leg etc.

Whilst staff are not expected to be experts or even knowledgeable in the identification of weapons and their legality, it is important that staff recognise that the availability of

weapons needs to be considered and evaluated as part of a risk management process, particularly if and/or when the individual experiences an exacerbation of their illness. Refer to Appendix 1.

The Weapons in The Community Policy supports staff actions when:

- They become aware that a service user has access to a weapon in the community
- The discovery of such items causes concern, which requires action

6.11 Security of Personal Property Belonging to Staff

Staff should remain vigilant and avoid bringing valuables to work and when possible secure personal property against loss. Where lockers are provided, they should be used and kept locked at all times.

6.12 Security of Service User Areas

Service user areas need to be welcoming and approachable to visitors and others; however the security and safety of service users must be the first priority of all staff. There must be a balance of security measures which also restrict access to intruders. Where possible, and with regard to fire escape requirements, service user care areas should be securely locked at night and staff should challenge all strangers. The vigilance of staff is a major defence.

6.13 Security of Patient Property

The loss of property can cause great inconvenience and stress to service users and can also lead to mistrust among staff. Service users should be persuaded, where possible, not to bring valuable items or large sums of money onto the premises. However where property is handed over safe keeping it should be managed in accordance with specific Trust policies relating to patient property.

- Each clinical area should have a safe, to store service users' valuable property i.e. money / jewelry.
- Each service user must 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 must not be stored on ward areas for more than 2 working days.
- Valuable item such as phones, rings / money must be stored on a longer term basis in the cash office or returned home.

6.14 Banned/Prohibited Items (CQC 2017)

All inpatient services will have some prohibited or 'contraband' items. However The Mental Health Act Code of Practice defines blanket restrictions as "rules or policies that restrict a patient's liberty and other rights, which are routinely applied to all patients, or to classes of patients, or within a service, without individual risk assessments to justify their application." The Code's default position is that "blanket restrictions should be avoided unless they can be justified as necessary and proportionate responses to risks identified for particular individuals". The Code does allow that secure services will impose blanket restrictions on their patients. The following are items that are typically banned in NHS inpatient services.

- Alcohol and drugs or substances not prescribed (including illicit and legal highs)
- Items used as weapons (firearms- real or replica, knives or others sharps, bats)
- Fire hazard items (flammable liquids, matches, incense)
- Pornographic material

- Material that incites violence or racial/cultural/religious/gender hatred
- Clingfilm, foil, chewing gum, blue tack, plastic bags, rope, metal clothes hangers
- Laser pens
- Animals
- Certain types of recording equipment

Where blanket restrictions are identified as necessary and proportionate there should be a system in place which ensures these are reviewed within a regular time frame, with an overall aim at the reduction of restrictive practices.

6.15 Restricted Items (CQC 2017)

Restricted items are items where the access is controlled and may be directed according to policy and individual risk assessment. Examples of items that may fall into this category include:

- Disposable cigarette lighters
- Toiletries- aerosols, razors
- bank cards, items of stationery
- Cutlery, tinned materials, glassware

Risk assessments and personalised care related to restricted items
Access to items will depend on many factors, some of which may be fixed and others subject to change. The risk assessment and ensuing management of access to security items should take a procedural and individualised approach, where possible in collaboration with the patient, which avoids the implementation of unreasoned blanket bans. For items that may be considered suitable only for restricted use, staff should complete a thorough risk assessment and provide the patient with a transparent rationale that explains the management outcome.

6.16 Illicit Substance Abuse

The LSMS/Divisional Security Lead Security will ensure that appropriate arrangements operate within their service areas to facilitate the confiscation of illegal substances from service users and visitors. Such arrangements shall include escalating drug issues to the appointed Mental Health Investigators; arrangements for securing and safe disposals of such articles.

6.17 Lost and Found Property

Service users, staff and visitors need to understand that the Trust take lost property seriously. All lost property incidents are to be investigated at ward/department level in the first instance and reported on an incident report form. Should it be identified that other Trust staff were responsible for the loss; affected staff are to seek advice from their manager regarding compensation for the loss. Any found property is to be handed in to the local office or reception for safe keeping.

6.18 ID Badges (Processing and management of consumables)

An Identification Badge (ID Badge) is an accountable document designed to establish the identity of the holder. All staff, volunteers and other authorised contractors/ visitors whilst on duty/and or visiting Trust premises must display an Identity Badge. This is particularly relevant in clinical areas where there is frequent contact with patients and the public. The security benefits of an ID Badge system are to:

- assist patients to identify members of staff, a need highlighted in the Francis Report;
- prevent and deter bogus medical officials or health workers from impersonating Trust staff;

- assist staff in confirming identification of other members of staff when handing over drugs, valuables and property and other material;
- distinguish easily Trust staff from the staff of other agencies, contractors, maintenance staff and visitors working on Trust premises.

Security of ID Badges

The security of access control Fob's and ID badge consumables must be maintained at all time by:-

- Ensuring that IT equipment and software used to create ID cards and authorise access is password protected.
- Ensuring that all consumables used in the ID badge making process is secured and not accessible to unauthorised personnel.

Lost ID badges:

At all times the following procedures must be adhered to:-

- Report lost/stolen ID badges to your line manager and Facilities who will cancel authorisation and access of the ID badge/fob.
- Complete an incident report via Datix
- Arrange replacement badge with Facilities or other responsible area

End of employment (Cleansing ID card database:

- At the end of employment it is the responsibility of the manager to retrieve the identification badge and arrange for its deactivation and destruction.
- Line manager must complete the leavers report form and return to Human Recourse.
- Facilities will check the leaver's reports weekly/monthly and cancel authorisation and access of each ID card.

Auditing of ID Badge Database:

The Head of Health Safety will undertake an audit of the ID card badge electronic database system to ensure that the system is cleansed of all leavers

6.19 Challenging Persons Not Displaying a Valid ID Badge

Any unescorted person who is seen not wearing a visible Trust ID badge whom is found in any non-public area should be challenged. A polite but assertive challenge should be all that is required for that person to identify themselves, such as, 'Can I help you?' Suspicious behaviour should be reported to your manager, LSMS and Divisional Security Lead.

6.20 Management of Keys & Security Fob Access/Egress

All Managers/Ward Managers and key holders are responsible for the management of security keys and access/egress fob's within their ward/department and at all times must ensure the following:

- That when staff, leave the Trust or move to another department that the key/fob and other security devices is retrieved from the staff member.
- Ensuring that key boxes/cabinets are kept locked at all times.
- That all security keys and fobs are tagged and numbered.
- That on shift handover all keys are signed in/out and accounted for.
- Undertake a monthly audit of keys and key signing in/out procedure.
- Ensure that missing keys are reported to the Security Manager and an incident

report raised via Datix.

- Undertake a full search for missing keys and risk asses the need to change all suited keys.
- That replacement keys and fobs are funded from the department's budget.
- Ensure that the code for digital locks are changed every six months

Each key holder (Secure Services) 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/Divisional Security Lead 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.
- 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.

6.21 Maintenance Work

Local managers must be notified by the estates department before starting maintenance or contract work e.g. window cleaning, electrical/plumbing. In secure mental health wards, the work should be closely supervised. All maintenance contractors in line with the Control of Contractor Policy must report to site in the first instance.

Local managers will ensure the security of patients, staff, equipment and property. This is particularly relevant in areas occupied by vulnerable patients and during the hours of darkness.

6.22 CCTV Procedures (extracting images)

Where staff have been authorised to access CCTV images as part of evidence gathering for both internal and external police investigations they shall:

- Ensuring that CCTV viewing and extraction of images remain compliant with the Data Protection Act.
- Refer all requests for images to the LSMS.
- Note that images or information related to these can only be released by the LSMS in line with the Trust CCTV Policy.

6.23 Car Parking and Vehicle Security

Car parking must be confined to the designated areas which are provided with lighting. The main points related to vehicle security are set out below:

- Lease car drivers must lock their vehicle and activate the security device/alarm in accordance with the instructions for use of the vehicle.
- Personal items and any Trust property must be removed from view when the vehicle is left unattended, thus limiting the possible risk of theft and damage to the vehicle.
- Staff should lock vehicles and where security devices are fitted to the vehicle then these should be activated

6.24 Managing Violent & Abusive Behaviour by Members of the Public

Whilst assuming a zero tolerance stance regarding violence and aggression is desired it has been accepted nationally that this is not realistic. However, the managers must consider all incidents individually and with particular sensitivity, taking full account of, and support for, the wishes of victims as much as it is reasonably practicable in the circumstances.

All line managers and departmental heads need to ensure the following actions are carried out for all activities and locations:

- Role based risk assessments – must be formally recorded in accordance with the Trusts Risk Management Policy.
- Implementation of risk mitigation/control measures, including staff training.
- The prompt reporting of ALL incidents of violence and aggression (verbal or physical).
- The wellbeing of the victim following an assault.
- All assaults on staff members are immediately reported to the police and the LSMS/Divisional Security Lead.
- That any member of staff who becomes a victim is fully supported and is referred for counselling – if necessary.

Part of the incident handling process should involve a root cause analysis and plans for prevention of repetition of the incident.

All employees must incorporate good working practices together with security measures as part of an overall requirement. The Trust will have systems in place to ensure an appropriate response to incidents including:

- Recording all incidents on Datix, whereby trends can be identified and risks assessed.
- Routine reports indicating trends and the needs for action to be taken in compliance with all relevant security policies

The Trust is committed to reducing aggression against its staff and will consider measures to achieve this including:

- Instructor lead training in Secuirty and Breakaway Techniques for all inpatient staff and staff with regular contact with the public who are in role identified as being in a moderate or high risk role based on a formal documented risk assessment;
- E-learning based training in Conflict Resolution for all other staff.
- The LSMS/Divisional Security Lead will speak on personal safety and security awareness at Divisional meetings and Team Training Days (as requested);
- On-going risk analysis by managers;
- Being supportive to staff identified as being at risk.
- Taking management action in line with the national framework of sanctions as produced by the then NHS Protect.

6.25 Staff Support Following an Incident or Near Miss

The Trust will fully support employees who report an incident. When an offence is committed against persons or NHS property within the Trust and the culprit is identified, it is the policy of the Trust to report the matter to the police and seek redress and/or sanction where appropriate.

A Datix report must be completed for all incidents or near misses. Employees are to report the full details to their appropriate manager/supervisor immediately before referral to any other agencies, e.g. Occupational Health, Human Resources, etc. (except in the case of incidents requiring an immediate Emergency Services presence or response).

The Trust provides staff with access to a counselling service. Following an incident, managers must ensure that staff members are given the opportunity to discuss the incident and receive assistance in the preparation of reports on the incident.

Managers must arrange for staff to have time off to attend supportive agencies if required. Staff may wish to consult with their trade union representative or LSMS/Divisional Security Lead to obtain further advice and assistance.

6.26 Post Incident Investigations

After any incident of violence or aggression against an employee, line and service managers are to ensure that a root cause analysis is conducted and that a copy of the Risk Assessment for the task which was being under taken by the victim at the time is immediately forwarded to the LSMS/Divisional Security Lead.

6.27 Lone Working

Working alone is not prohibited by health and safety legislation and it will often be safe to work in this way. However, the law requires employers to consider carefully, and then deal with, any health and safety risks for people working alone.

The broad duties of the Health and Safety at Work Act 1974, the Management of Health and Safety at Work Regulations 1999, the Corporate Manslaughter and Corporate Homicide Act 2007, the Safety Representative and Safety Committees Regulations 1977, the Health and Safety (Consultation with Employees) Regulations 1996, apply.

These require the identification of hazards associated with lone working, assessment of the risks involved and putting in place measures to avoid or control the risks.

6.28 Lone Worker Risk Assessments

Risk assessments must be carried out by line managers with all staff as part of the induction process. The assessments must be recorded, re-examined at regular intervals and communicated to all who could be affected or identified by the risk assessment.

Re-assessment must take place annually as a matter of routine; more frequently in the event that there is a significant change in the individual's role and responsibilities, work base or disability / health status.

Measures to control the risks should take account of normal working conditions and foreseeable emergency situations such as fire, equipment failure, illness and accidents. When considering safe working arrangements, line managers should follow a hierarchical system based on the following:

- Identify who is operating as a lone worker;
- Identify any possible risk(s);
- Assess the likelihood and consequences of each risk;
- Avoidance of the risk where possible;
- Control of the risk as far as reasonably practicable;
- Evaluation and review of the effectiveness of control measures.

6.29 Failure to return/respond to attempts to contact a lone worker

Where staff attempt to make contact with a lone worker and there is no response, or, where a lone worker fails to return as expected, the following action is to be taken:

- Leave Voice message if possible requesting urgent contact.
- After 15 minutes with no response escalate to head of department,
- Call home address and enquire after colleague – do not hint at any problems.
- Manager to contact On Call Director.

- Make decision to call police.

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.

6.30 Visitors/Contractors

All contractors and visitors to Trust premises for business purposes should be signed in and out of the premises. There will be a visitor log held at the reception area. The member of staff who is responsible for the visitor/contractor will then arrange for the visitor to be escorted at all times whilst on the premises.

6.31 Search Process (Visitors)

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.

6.32 Reporting of Incidents

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/Divisional Security Lead within 24 hours of the incident occurring.
- If IT equipment is stolen and potentially contains confidential material The Data Protection Officer should be informed.
- 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/Divisional Security Lead against number and type of incidents reported with the aim of identifying gaps in incident reporting.

6.33 Lockdown

The aim of a lockdown is to exclude or contain people by preventing entry to, exit from, or movement around a building or site. In some cases lockdown of individual buildings within a larger site may be required. This is required as a response to a threat or emergency which may endanger the wellbeing of service users, staff or visitors.

This threat could range from any of the following listed below. Each Trust property or site should be capable of quickly achieving a partial or full lockdown in the event of any given emergency.

Incident	Action	Lockdown
Bomb threat/ Suspicious package	Isolate and call police	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
Terrorist on site	Call police	Yes
Chemical/biological contamination	Call emergency services	Yes

Lockdown arrangements will vary in complexity depending on the size of the premises and the scale of the emergency. For each property an assessment will be made on the capacity and capability to lockdown, which will feed into the creation of robust lockdown procedures for that property.

The level and robustness of the lockdown will be dependant on a variety of factors and a specific lockdown risk profile is required. The lockdown risk profile is to be completed by the service manager, with the advice of the Safety Team.

6.34 Counter Terrorism

Whilst there is no evidence to suggest that the NHS is any more at risk from terrorism than other public service organisations, however staff should maintain a level of alertness. Counter terrorism guidance can be found on the MI5 and Centre for Protection of the National Infrastructure websites. www.mi5.gov.uk and www.cpni.gov.uk

6.35 PREVENT

Should any member of staff have concerns relating to an individual's behaviour which indicates they may be being drawn into terrorist-related activity, they will need to take into consideration how reliable or significant the indicators are.

All staff must raise their concerns through the PREVENT Lead and the Trust's Safeguarding Team and seek advice on how to address them in accordance with NHS PREVENT.

Staff must seek advice through the Trust's Safeguarding Team, and out of hours advice can be sought via the Trust's On Call Director.

Where staff believe concerns may need to be escalated, the PREVENT Lead and/or the Trust's Safeguarding Team will assist in determining whether the matter needs to be referred on.

6.36 Telephone Bomb Threats

Making such malicious calls is an offence contrary to Section 51 of the Criminal Law Act 1977 and should always be reported to the police. The procedure listed below must be used in event of the any Trust location receiving such a call:

In all cases it is important to telephone the police immediately with details of the call. The message may be brief and the caller may ring off before detailed information can be obtained. However, try and obtain what information you can, such as detailed in the Premises Security Plan. The four key rules are:

- Keep calm.

- Try to obtain as much information as possible from the call.
- Keep the line open even after the caller has hung up.
- Report the call to your manager.

This is easier said than done. Do not underestimate the stress of receiving a threatening call - it can put the best intentions out of mind until the caller has rung off and it is too late to try to get more details.

If at all possible, the person receiving such a call should signal to a colleague to listen in on the same extension. Another person listening on the line may help to remember important facts afterwards.

- Keep the caller talking for as long as possible.
- Try to ask questions in sequence using as natural a voice as possible.
- Remember **DON'T HANG UP**

6.37 Police Liaison (Mental Health Investigators)

The Trust contributes to the joint funding of a Police Constable (PC) who acts as specialist Mental Health Liaison Officers 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.

The work of the Police Liaison Officer is coordinated jointly by line managers the LSMS and Divisional Security Lead. 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

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

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.

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 Information Security and Data Protection

The aims of information security and data protection are to preserve confidentiality that is, protecting information from unauthorized access and disclosure with the following requirements:

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

7.0 CONSULTATION

7.1 The Trust will ensure that all members of staff are provided with the information that they require to work safely and without risk to their health. This will include information, such as the results of assessments and the appointment of various categories of competent persons, required under various pieces of legislation.

7.2 Consultation on health and safety matters with employees who are members of a recognised trade union will take place through the agreed channels. However; employees who are not members of a recognised trade union will be consulted with either directly or through a representative whom they have elected. This will enable the trust to meet its obligations under the Consultation with Employees Regulations 1996.

8.0 TRAINING AND SUPPORT

What training	How delivered	Which staff group	Frequency	How monitored	Escalation of non compliance
Key Security	Face-to face	High secure	At induction	Learning development training data	Safety committee
Security/Conflict management	Face-to face E-learning	Clinical staff	At induction 3 year update	Learning development training data	Safety committee
Use of lone working devices	Face to face	Staff assessed as lone workers	Induction and as required	Health and safety team training data	Safety committee

9.0 MONITORING

Criteria	Monitoring Mechanism	Responsible	Committee	Escalation	Frequency
Security Risk Assessment	Risk assessment audit	Health & Safety Team	Health and Safety Committee	Quality & Assurance Committee	Annually
Ward Management of keys and security fobs	Workplace Inspections	Health and Safety Team	Health and Safety Committee	Divisional Surveillance	6 monthly
Security	Review of	Health and	Health and	Security	Quarterly

incidents, risks and breaches	Datix reports	Safety Team	Safety Committee	Group	

10 Appendices

- Appendix 1: Weapons in the community
- Appendix 2: Security Risk Assessment
- Appendix 3: Principle of Crime Prevention
- Appendix 4: Lockdown Practices
- Appendix 5: Equality Human Rights Analysis

Appendix 1

WEAPONS IN THE COMMUNITY

Section 1- General Guidance

This Policy and Procedure is aimed at providing direction to staff as to how the potential risk of individuals having access to weapons should be considered and managed in a measured way.

It is recognised that staff are not expected to be experts or even knowledgeable in the identification of weapons and their legality. It is important that staff recognise that the availability of weapons needs to be considered and evaluated as part of a risk management process, particularly if and/or when the individual experiences an exacerbation of their illness.

This appendix has been drawn up to support staff actions when:

- They become aware that a service user has access to a weapon in the community
- The discovery of such items causes concern, which requires action

It is recognised that each case is different and the response will have to be individually considered, taking into account the context of the situation. Reporting to the police may not lead to any direct action form them, but could and should provide the care team with advice and guidance as to how to manage the situation.

It is recognised that any object involved in threat or attack can be described as a weapon and commonly include knives, broken glass, needles and other sharp objects. Also seemingly innocent household items could easily be utilised to threaten or cause injury e.g. Cutlery, baseball bat, chair leg etc.

This guidance relates specifically to the observation of more clearly defined and specifically manufactured weapons (even if made by the individual owner). This is important as even non-threatening carriage of these items, could cause members of the public to be concerned and call the Police this creating a danger/distress for the service user.

- An **OFFENSIVE WEAPON** is legally defined as any article made or adapted for use to cause injury to a person, or intended by the person having it with him for such use.
- A **FIREARM** is a lethal barrelled weapon of any description from which any shot, bullet or other missile can be discharged.
- An **IMITATION FIREARM** means anything, which has the appearance of being a firearm.
- **PROHIBITED WEAPONS** include any air-rifle, air gun, air pistol which uses or is designed or adapted for use with a self-contained gas cartridge system.
- **KNIVES**- It is an offence to be in possession in a **public place** of any article, which has a blade or is sharply pointed (including a folding pocket knife if the cutting edge of its blade exceeds 3 inches). This covers all designs of bladed object, whatever its original function.

In the home consideration should be given to blades in an unexpected or unusual place. For example a kitchen knife placed on a fire surround or sideboard, or a craft knife on a surface when no craft items around. This may indicate a threat exists and staff should act accordingly.

WHEN URGENT ACTION MAY BE NEEDED

This is more often where the member of staff observes a weapon and feels under threat, or others are at risk. Also, any firearm which is not securely stored should be considered as an imminent risk unless other factors reduce the risk. If an imminent risk is perceived, the following actions should be undertaken.

Upon finding, suspecting or being told that a service user has a weapon/s the staff should:

- Remove themselves and where possible others to a safe place.
- Phone 999 immediately and provide the police with as much information as possible (it is essential that as mulch accurate information regarding individual, risk, weapon, potential victims etc., is shared. This will be used to grade/prioritise the police response).
- Follow safety instructions provided by police.
- Inform Line Manager /On Call Director
- Complete a Trust incident form
- Complete an entry in the patient's notes
- Place an alert/warning on the clinical records system

WHERE NON-URGENT ACTION IS NEEDED
This is where staff have recognised that the service user has access to weapons but where there is no perceived immediate threat to self/others.

- Consider discussion with service user, as there may be an explanation what will inform future actions and decisions.
- Identify and record the situation in which the weapon was found i.e. in a locked cupboard, on coffee table, used as an ornament.
- Assess the current mental state of the service user who has access to the weapon, paying particular attention to any imminent risk factors associated with the weapon.
- The decision as to how to manage this situation should be taken within the multidisciplinary team. If it is not possible to convene a full meeting, the discussions with team members should take place to ensure:-

- Actions agreed are representative of all staff involved.
- All staff are aware of their responsibilities, in relation to the agreed action.
- Risk of a public safety concern is considered objectively.
- Complete an entry in the patient's notes.

RISK ISSUES TO CONSIDER
The multi-disciplinary team should consider the issues below in order to identify whether there is a public safety issue. The risk issues identified are not prescriptive or exhaustive but will help facilitate a full consideration of the risks.

- Is the weapon safely stored/secured?
- Is the item accessible by children or other vulnerable people?
- Would an exacerbation of the individual's illness-question the rational use of the weapon.
- Is there a history or potential history (if the person is unknown to the Trust) of the service user misusing weapons in the past?
- Has the individual previously shared ideas/thoughts of injuring people in using any method?
- Is the access to a weapon a new pattern of behaviour and associated with their symptoms of mental illness i.e. increasing level of paranoia.
- Have the service user's family/carers raised concerns about access to /storage of weapons?

NO IMMINENT PUBLIC SAFETY CONCERN
If the team do not access that a public safety issue exists at this point, then the following should be undertaken/considered:

- Formally risk assess the situation and includes actions and decisions within clinical records.
- Discuss any concerns and management arrangements with service user.
- Advise service user on how they can gain advice/guidance on Safe management of their weapon.
- Advise service user on why removal/disposal would be appropriate.
- For all firearms, prohibited firearms and offensive weapons the police should be informed. Staff should lead a discussion with the police concerning our need to maintain a relationship with the

service user, and request sympathetic, but appropriate, action by the police which maintains a supportive role. This action is supported by Section 29 of the Data Protection Act and /or Section 115 of the Crime and Disorder Act.
- Advise service user on requirements regarding storage during community visits.
- Continue to review risks associated with weapons.
- Agree protective measures for future contacts i.e. location of visits, numbers of staff to attend, etc.
- Place an alert/warning on the clinical records system

PUBLIC SAFETY CONCERN
If the team believe that a public safety issue exists, then it is clear that staff can and should share concerns with the police with the aim of:-

- Clarifying natures of weapons and its/their risk.
- Providing formal guidance to the service user regarding storage/legality of ownership.
- Facilitating potential removal.
- For Mental Health Services, and where appropriate, Developing use of a Multi-agency Public Protection Arrangements (MAPPA) Processes.
- Where possible/appropriate the service user/carer should be informed of the care- teams concerns, and the requirement to inform the police for advice and guidance

The Information Governance of sharing information in this context is covered within the Data Protection Act (section 29) and the Crime and Disorder Act (section 115).

Both acts allow for such information to be shared between agencies. Further guidance can be sought from the Information Governance Team. The police will make a decision which will be based on the information provided and any other information available that is reasonable, proportionate and justifiable as to what action is required. Once the initial need has been identified to report to the police, a full discussion of the situation and clinical implication should be taken within a multi-disciplinary meeting. The risk management plan/care plan should be amended to take into account any newly assessed risks.

N.B. Staff must NEVER handle or take possession of anything, which is or looks like a firearm. Staff should only take other weapons away for service users with their permission. Disposal of any weapons should be via the nearest local police station unless local agreements dictate another course of action.

RECORDING INFORMATION
All actions, discussions and/or meetings will be recorded as soon as possible. The content of all informal discussions with the police will be logged by the police for audit and informing future risk assessments.

Within documentation the team needs to show that it has considered whether the availability of the weapons will or could constitute a public safety issue. As previously stated this relates to the risk that his individual may pose to others or them-selves and the risk the availability of the weapon by others may pose. Issues to consider:-

- Previous history of violence.
- Previous history of using weapons.
- Concerns for children and vulnerable adults who may be in the home or come into contact with the weapons.
- Concerns from family/carers regarding a new and unusual interest in and /or collection of weapons.
- Stability or mental health and symptoms associated with violence to self or others
- Evidence of ‘Substance Misuse.

SEEKING ADVICE/GUIDANCE

The identification of a public safety issue is not always easy or clear: it is recognised that teams may require assistance to make a decision that is rationale and measured.

It is recommended that where different views are held by team members or the discussion is not clear then advice and guidance should be sought. This can include involvement of the police at an advisory level or provision of a legal opinion. On other occasions, it may be simply a case of accessing a third party opinion that will help add objectivity to the proceedings.

POTENTIALLY OFFENSIVE WEAPON IDENTIFIED	
URGENT ACTION IS REQUIRED	**URGENT ACTION IS NOT REQUIRED**
Risk is very high	**No obvious immediate risk**
1. Move to a safe place 2. Phone 999 immediately (or activate Lone Worker Device if available) and 3. provide the police with as much information as possible 4. Inform Line Manager/Manager on-call 5. Complete a Trust incident report 6. Complete an entry in the service user record.	1. Consider discussion with service user. 2. Identify and record the situation in which the weapon was found. 3. Assess the current mental state of the service user who has access to the weapon, paying particular attention to any imminent risk factors associated with the weapon. 4. Convene a multi-disciplinary meeting, or at least speak to the team leader and colleagues 5. Decide if there is a concern for public (or staff) safety and complete and make entry in the service user record.

POTENTIALLY OFFENSIVE WEAPON IDENTIFIED	
PUBLIC SAFETY CONCERN	**NO PUBLIC SAFETY CONCERN**
If the team believe that a public safety issue exists, the it is clear that staff should share concerns with the police with the aim of : 1. Clarifying the nature of weapons and their risk 2. Providing formal guidance to the service user regarding storage/legality of ownership. 3. Facilitating potential removal. 4. Where appropriate the service user should be informed of the care- teams concerns and the requirement to inform the police. 5. Complete an entry in the service user record.	If the team do not assess that a public safety issue exists: 1. Formally risk asses the situation. 2. Discuss any concerns and management arrangements with service user. 3. Advise service user on how they can gain advice/guidance on Safe management of their weapon. 4. Advice service user on why removal/disposal would be appropriate. 5. For all firearms, prohibited firearms and offensive weapons the police should be informed. 6. Continue to review risks associated with weapons, complete an entry in the service user record.

Appendix 2

Security Risk Assessment

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.

Location/Address		
Building Manager		
Assessor(s) name		
Assessment date		
Description of building and service being delivered		
Crime profile of geographic area (LSMS to assist)		
List of reported security incidents	Brief description of incidents	Police involved Yes / No
Contracted security services (e.g. static/mobile guards		

Security Profile (External)		Yes	No	N/A	RAG Rating
1	Are external areas and car parks covered by adequate lighting?				
2	Are external areas covered by CCTV?				
3	Are CCTV systems inspected and tested annually by a contractor?				
4	Is the CCTV system and cameras in good working condition?				
5	Is CCTV signage displayed at the entrance of building or when entering site?				
6	Are security doors in good working condition				
7	Are waste material contained in secure location?				
8	Are there any vulnerable points where potential offenders could hide e.g. behind high bushes in concealed door ways etc?				
9	Are there areas where staff might feel isolated?				
10	Are there any potential climbing points such as pipes or flat roofs				
11	Are premises and security doors in good repair?				
12	Any reports of acts of vandalism				
13	Are mobile / static security guards used on site				
14	Are visitors encouraged to use the main door and is this clearly signposted?				
15	Is there a keypad system/digilock in use to control access and egress?				
16	Is there an intercom system in place				
17	Is there an established procedure for locking up?				
18	Is there allocated parking areas for staff?				
19	Is there clear access for emergency vehicles and personnel outside the building?				

Observation:

Security Profile (internal)		Yes	No	N/A	RAG Rating
1	Is the premises protected by CCTV e.g. reception, corridors etc				
2	Is the CCTV system password protected?				
3	Is the building protected by an intruder alarm?				
4	Is the intruder alarm linked to a receiving center who respond to alarms?				
5	Is the building fitted with a staff attack system?				
6	Are panic buttons fitted at reception or vulnerable areas?				
7	Are panic alarms tested weekly/monthly by staff to ensure they work?				
8	Are panic alarms tested and inspected annually by MITIE?				
9	Is a recognised staff response procedure on activation of an alarm?				
10	Are windows restricted to 100mm and in good repair?				
11	Are controlled drugs and prescription pads stored securely?				
12	Are staff aware of data protection and the need to keep patient identifiable information safe and secure				
13	Are their high numbers of people who might access the building during the day?				
14	Is the waiting area supervised?				
15	Are there posters and information clearly in place – advising how to obtain entry and exit?				
16	Are visitors escorted to their destination?				
17	Do staff challenge strangers whom they see in the building?				
18	Are tools and ladders locked securely away?				
19	Is the MHA Tribunal Room fit for purpose (design, layout, panic alarm?				
20	How does the unit control prohibited items coming into the unit. Is this adequate?				
21	Does the unit use passive/active search dogs?				
22	Are staff aware of the Search Policy and when to use it?				

Observation:

Access Control		Yes	No	N/A	RAG Rating
1	Are physical access control measures in place denying access to staff only / unauthorised areas				
2	Are codes for key pad/digital lock systems changed every 6 months				
3	Are security doors locked and not wedged open				
4	Are ID cards/lone working devices recovered as part of the final the final interview process (documentary evidence to be provided)				
5	Are ID cards / access control fobs cancelled for staff on long term sick				
6	Has the access data base been cleansed of Trust leavers (check with system administrator)				
7	Is there a signing in procedures at reception				
8	Is there a signing procedures for visitors at the point of entry on to wards				
9	Are contractors allowed to sign out security fobs and enter a ward? (security fobs should not be made available to contractors)				
10	Are Visitor's badges given to non-Trust staff?				
11	Is the reception area at a height to deter service users' jumping over?				
12	Do the reception staff have clear sight lines to identify which service users are coming into the building?				
13	Do the reception staff know how to call and when to summon the police?				
14	Is there controlled egress and access into the reception area?				
15	Are staff offices and toilets locked?				
16	Is furniture fit for purpose and adequately secured to prevent barricade and assault?				
17	Are doors designed to prevent absconsions?				
Observation:					

Security Key Management		Yes	No	N/A	RAG Rating
1	Is there a key signing in/out book and is it is up to date with a return signature (check to see if staff have signed out keys)				
2	Are all key sets tagged and numbered and kept in a secure box etc?				
3	Have staff received key security training				
4	Are all security keys/fobs accounted for at the end of shifts				
5	Is there evidence that keys are not been signed in/out?				
6	Is there evidence of security keys/fobs leaving the building/ward				
7	Is there enough security keys for staff on shift?				
8	Have staff been informed not take keys home or keep as their personal set?				
Observation:					

Staff Security Training and Awareness		Yes	No	N/A	RAG Rating
1	Have staff completed MVA / break away training?				
2	Have staff been trained in use of staff attack system?				
3	Have lone working risk assessments been completed?				
4	Have lone working devices been issued?				
5	Have lone working been provided with a mobile?				
6	Are details of lone workers held to line managers?				
7	Is there a 'buddy' system in place for lone workers?				
8	Is there an up to date location board of lone workers?				
9	Is there an escalation procedure if lone workers are can not be contacted?				
Observation:					

Lockdown Procedures		Yes	No	N/A	RAG Rating
1	Has a local lockdown procedure been developed and tested for the building?				
2	Are staff aware and provided with details of the lockdown procedures?				
3	Are there any reasons why the building could not be secured by lockdown?				
4	Are security services required to assist with a lockdown ?				
5	List Observation:				

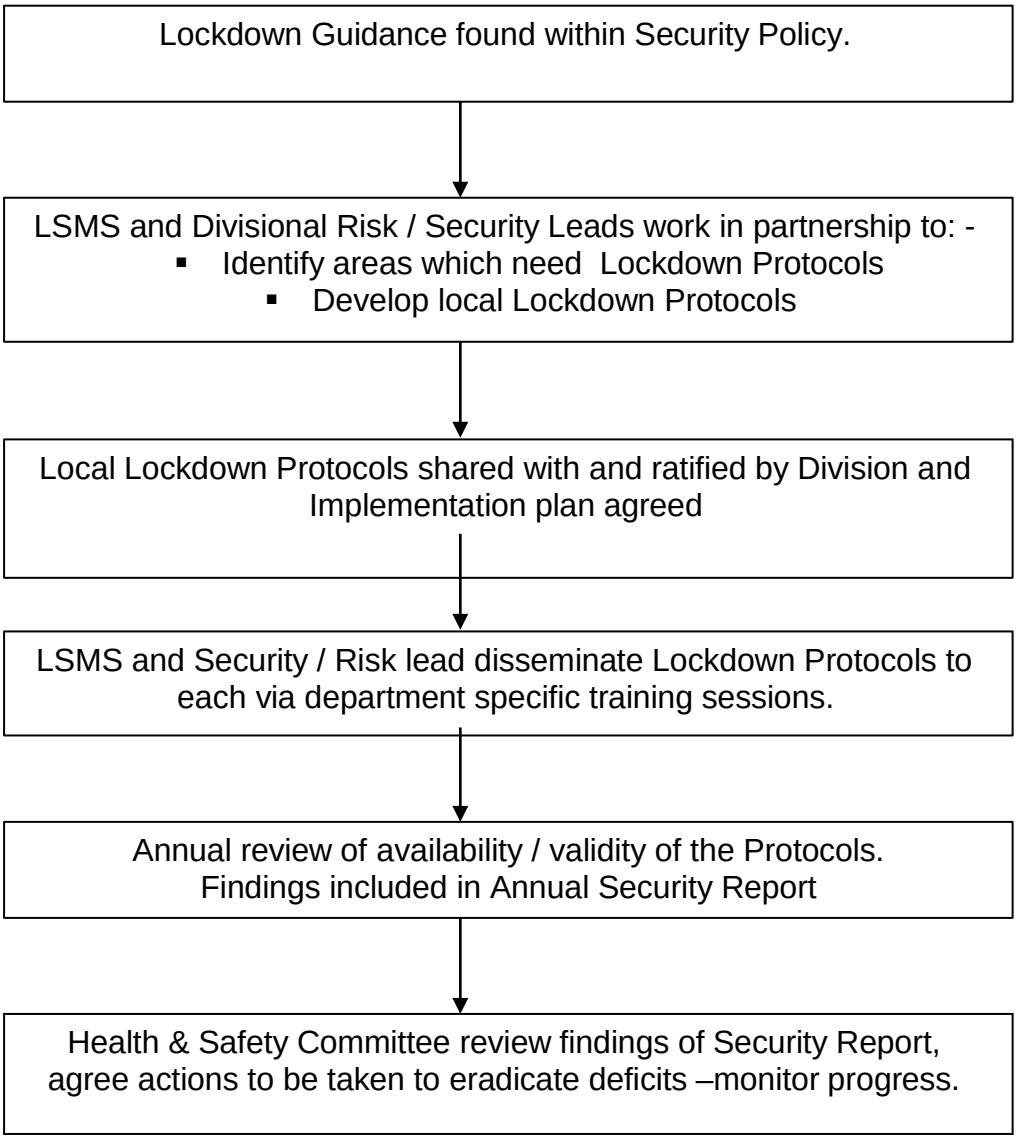
ACTION PLAN

Issues identified in the observation reports should be listed in the action plan for remedial action

	Issue	Action required	Lead	Timescale	Progress Update	RAG Rating
1						
2						
3						
4						
5						
6						
7						

Appendix 3

Development of Lockdown Protocols



Appendix 4:

Equality and Human Rights Analysis

Title: THE MANAGEMENT OF SECURITY SYSTEMS (SA29)
Area covered: Trust wide

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 safe secure and 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 shared with and agreed by the Health and Safety Committee

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
Head of Health Safety Fire & Security

Date assessment completed:
22/01/2020

Name of responsible Director:
Executive Director of Communication and Corporate Governance

Date assessment was signed: 22 / 01 / 2020