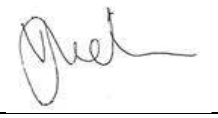
Birmingham and Solihull Mental Health NHS Foundation Trust

SECURITY POLICY

Policy number and category	**R&S 25**	**Risk & Safety**
Version number and date	**5**	**January 2021**
Ratifying committee or executive director	**Clinical Governance Committee**	
Date ratified	**February 2021**	
Next anticipated review	**February 2024**	
Executive director	**Director of Operations**	
Policy lead	**Local Security Management Specialist**	
Policy author *(if different from above)*		
Exec Sign off Signature (electronic)		
Disclosable under Freedom of Information Act 2000	**Yes**	

POLICY CONTEXT

The Board recognises that security management is an integral part of good, effective and efficient risk management practice and to be effective should become part of the Trust's culture and strategic direction.

POLICY REQUIREMENT

- How to maintain a safe and secure working environment
- Who to seek advice from in relation to security risks
- The management of security related contracts
- Determine Security Local Operating Procedures

CONTENTS

Introduction

1.1 Rational

1.1.1 The aim of this policy is to describe the framework for the management of physical safety and security of staff, service users, visitors, public, premises and assets of Birmingham and Solihull Mental Health NHS Foundation Trust (BSMHFT). It details the areas to be covered, the responsibilities of groups and individuals, and the processes to be followed.

1.2 Scope

1.2.1 This is a corporate policy that applies to all employees of BSMHFT, including contractors, employees of other organisations working within the Trust, seconded staff and volunteers. BSMHFT staff employed within Prison Healthcare Services are specifically excluded from this policy, as they will be required to adhere to policies specific to the Prison Service. However, all staff, including those working in Prison Healthcare are expected to report security related incidents via the Trust incident reporting process (ECLIPSE).

1.3 Principles

1.3.1 This policy has been developed to provide a safe and secure environment for service users, visitors and staff. The policy defines security objectives, sets out arrangements for achieving them and identifies key responsibilities for ensuring the policy is effectively implemented.

1.3.2 The Trust positively supports individuals with learning disabilities and ensures that no-one is prevented from accessing the full range of mental health services available. Staff will work collaboratively with colleagues from learning disabilities services and other organisations, in order to ensure that service users and carers have a positive episode of care whilst in our services. Information is shared appropriately in order to support this

2. Policy

2.1.1 Every member of staff must be aware of their security responsibilities in the context of this policy and take appropriate measures for the safety of themselves, service users, visitors and members of the public. To achieve this, tripartite arrangements based on integration of three key elements of security management are used which are:

- **Relational Security** is the knowledge and understanding staff have of a patient and of the environment, and the translation of that information into appropriate responses and care.
- **Procedural Security** is the use of policies, practices or guidelines for controlling, mitigating and managing identified security risks. As opposed to other means of control, procedural controls rely on users to follow rules or perform certain steps that are not necessarily enforced by technical or physical means.

- **Physical Security** relates to the specification of the building including (but not exclusive to) CCTV, fencing, doors, walls, ceilings, locks and windows and the general fabric of the building and its design.

2.1.2 To support each of these elements, each Trust building/hub will be equipped in accordance with the specific guidance issued by the Department of Health in relation to the appropriate security systems required for the various categories of psychiatric in-patient units as follows:

- **Adult Acute and Rehabilitation Inpatient Units:** Department of Health, Health Building Note (HBN) 03-01: Adult Acute Mental Health Units' (2003).
- **Adult PICU:** Additional Guidance to National Minimum Standards for General Acute Services in Psychiatric Intensive Care Units (PICU) and Low Secure Environments' (2002).
- **Low Secure Unit:** Royal College of Psychiatrists' 'Standards for Low Secure Services' (2012).
- **Medium Secure Units:** Department of Health, Environmental Design Guide 'Adult Medium Secure Services' (2011).

2.1.4 Individual members of staff will respond to and report security risks and incidents as they become aware of them, using the Trust incident reporting system, ECLIPSE. Staff with managerial responsibilities will ensure that all security related risks when notified, are assessed, documented, and communicated and that all possible actions are taken to mitigate such risks. All actions taken should also be updated on the appropriate ECLIPSE incident report. Divisional/programme risk registers will also record security related risks.

3. Procedure

3.1.1 To provide and maintain an environment that is safe and secure, this overarching policy requires that the following processes and security measures be followed and implemented in a manner that is commensurate with the services provided at that location:

- Trust sites/hubs will have an annual Security Risk Assessment (appendix 2) completed by the Trust Local Security Management Specialist (LSMS), to identify and assess requirements required for each locality/service.

- Security Staff where deployed as part of the Trust's PFI contractual agreements, will provide support through a managed security service undertaking general security duties in accordance with the specific Security Service Level Specification agreed via the Trusts' partner PFI providers.

- A list of contraband items (Appendix 4) will be made available detailing items that are not allowed to be brought into Trust buildings at the point of entry.

- All persons entering a Trust building should be prepared that they may be subjected to security checks to ensure that items deemed as contraband (Appendix 4), are not taken into clinical areas. Depending on the location, such checks may by undertaken by Trust staff and/or contracted security officers. Anyone not consenting to these checks will be refused entry to the building.

- In the event a returning service user does not consent to a security check on entering a building, the relevant ward/clinical team will be contacted and asked to attend and escort the service user to the clinical area where the Searching of Service Users Policy (RS 45) will be implemented.

- Security checks may be undertaken visually, and/or with the use of passive electronic monitoring/detection equipment. Information signs will be installed on the approach to and within entrances alerting users of the building that such equipment is installed and that such checks may be undertaken of bags and items which are brought in.

- Trust sites will have perimeter fencing that is commensurate with the service provision and constructed in accordance with the appropriate Department of Health Guidance.

- Access control systems to prevent unauthorised access and visitor management systems (electronic or signing in/out), that are commensurate with the security requirement of the location.

- Following appropriate risk assessment criteria and a requirement identified, anti-barricade door sets fitted to areas where service users, visitors and the public have access,

- Following appropriate risk assessment criteria and a requirement identified, remote staff assistance alarm system will be installed to all rooms, courtyards, corridors, toilets etc. to which service users, visitors and the public have access.

- Assistance Alarm Systems must be supported by a documented alarm activation response protocol and equipment testing process.

- Where staff assistance alarms are installed, staff will carry assistance alarm fobs whilst on duty.

- All Trust staff will wear Trust Identification badges whilst on Trust premises. The only exception being where staff exchange their ID for keys or where biometric identification systems are in place to verify the identity of staff entering Trust buildings.

- Following appropriate risk assessment criteria and a requirement identified Trust sites/hubs will be equipped with CCTV systems and appropriate warning signs installed.

- Following appropriate risk assessment criteria and a requirement identified reception areas will be equipped with security screens for the protection of staff.

- All reception areas will have a Safety Information Board for Staff and Visitors with the day & date and following information:

    - Senior Manager name and number
    - Incident Manager name and contact number
    - Staff Assistance Alarm Test today - Time
    - Fire Alarm test – day/Time
    - Evacuation Assembly Point
    - First Aider Name and number
    - Fire Evacuation Actions

- All receptions, waiting areas and consulting areas will be furnished with appropriately weighted furnishing to mitigate its use as a weapon.

- For Trust buildings that do not operate on a 24/7 basis, the locking and unlocking procedures must be undertaken by a minimum of two Trust staff (manager and/or nominated staff or contracted security officer(s) where an opening/securing service has been engaged). Facilities staff are not authorised to undertake this role and must not be tasked with the opening and/or securing of Trust buildings. This incorporates the activating or deactivating building security alarm systems

- Where an intruder alarm is installed all ground floor access points, including fire doors must be included within the zoning. All offices/rooms with external windows must be fitted with passive infra-red (PIR) sensors, including first floor areas. Where fitted, all intruder alarms within Trust buildings must be subject to an annual maintenance schedule and a record of such maintenance retained locally for inspection.

- External approaches, perimeters and car parking areas will be equipped with appropriate lighting.

- All windows must be closed when leaving a room unattended and items of value locked away.

- Where security codes are used, these must be changed at least every six months or whenever it is believed that the code has been compromised e.g., staff dismissal or high numbers of agency/bank staff. A local record of these changes must be retained by the responsible manager and held securely.

- No Tailgating – staff with access to secure areas must ensure that no unauthorised persons gain entry through tailgating. This is the process of allowing someone to follow you through a secure door or the holding open of a door for someone to enter a restricted area.

- Unauthorised or unknown persons in the workplace must be challenged where safe to do so and be able to produce a valid Trust photographic ID card or visitor pass where used. If it is not safe to challenge an unknown person, they must be immediately reported to a manager and/or security where present.

- Portable devices, such as Blackberry phones, mobile phones and laptops etc must be secured in line with the Trust Mobile Phone and Handheld Computing Device Policy (CG12), Remote Working and Remote Access Policy (CG20) and Information Communication and Technology Policy (IG02). All staff must ensure that their workplace is secured at the end of the working day (where applicable e.g., for sites that do not provide out of hours services) and that departmental keys are always held in a secure place.

- It is the responsibility of each department manager to ensure that their staff have a valid Trust Photographic ID card and name badge, and that these are worn appropriately.

- New Staff joining the Trust will complete an application for and be issued with their photographic ID as part of their Trust induction process.

- All staff have responsibility for the security of Trust Photographic ID cards, keys and personal issue staff assistance devices issued to them.

- All loses of these items must be immediately reported to line managers. Any failure to report such a loss in a timely and prompt manner may result in disciplinary procedures being considered by line managers.

- Where loses of Trust Photographic ID cards have been reported, where such cards have associated door access control functions, line managers must ensure such cards are immediately removed from the associated door control systems.

- An Eclipse form must be completed by the person whose card, keys or assistance alarm fob has been lost.

- Line managers will arrange for the lost card to be replaced and authorised with the appropriate access levels.

- Managers are responsible for ensuring that ID cards, name badges, swipe cards and keys are retrieved from any employee who is leaving the Trust through retirement, suspension, dismissal or serving notice to terminate employment.

- A risk assessment must be undertaken by the LSMS for all new construction and modernisation projects of Trust premises to ensure the correct level of physical security measures are incorporated.

3.1.2 Governance

3.1.3 Security Management will be monitored on a quarterly basis via the Trust Health, Safety Committee. The LSMS will prepare and submit a report to this committee to ensure the Trust receives the necessary assurances.

3.1.4 Each Trust site/hub will have a security inspection assessment undertaken by the Local Security Management Specialist annually or as a result of a specific incident and/or service request. An example of which is at Appendix 2.

3.1.5 The completed security risk assessment report, together with any recommendations, will be issued to the appropriate management team. All identified risks should be reflected in the relevant operational risk register. The management team, in co-operation with the relevant Estates Team and the LSMS, will formulate and produce an action plan as to how the identified risks are to be rectified or managed (Appendix 2). The relevant service management team are to ensure that recommendations within these plans are implemented or managed as appropriate. Within corporate areas of the Trust, such as B1, this responsibility would be that of the nominated building manager. All such action plans will in turn be monitored by the LSMS via the Trust Health and Safety Committee to ensure that highlighted risks are being managed or addressed. Where it is not possible to make physical changes to the mitigate identified risks, or there are delays with the implementation of changes, such risks should be recorded on the relevant service risk registers.

3.1.6 Lockdown

3.1.7 A lockdown is essentially an appropriate response to a variety of threats and hazards and is achieved through a combination of physical security measures and the deployment of appropriately trained staff.

3.1.8 Lockdown is part of the emergency planning process and forms part of the Trust Major Incident Plan. Procedures & guidance for the implementation of a Lockdown can be found at Appendix 3

4. Responsibilities

Post(s)	Responsibilities	Ref
Chief Executive	The Chief Executive has overall responsibility for the effective implementation of this policy.	
Clinical and Corporate Directors, Clinical Service and Nursing Managers, Ward/Team Managers, Advance Nurse Practitioners	In relation to the three key elements of security management, Associate Directors of Operations have responsibility for Relational and Procedural security. Physical security will be the responsibility of the Associate Director of Estates & Facilities. CNM's, service and nursing managers, have overall responsibility for the implementation of action plans, management of identified risks, and where	

	necessary the updating of the appropriate service risk registers.	
All Staff	All staff have individual responsibility to ensure that security and safety is always maintained whilst on Trust premises or working in community settings away from Trust sites. Where an incident occurs, all staff have a responsibility to document and follow the incident reporting process (Eclipse), in accordance with Trust Policies and Procedures.	
Policy Lead	The LSMS is responsible for the content of the policy and that the processes therein are followed. The LSMS will also provide support to colleagues in response to security related incidents. Conduct annual security risk assessments and formulate recommendations based on the findings of these audits. Provide additional support where criminal behaviours are identified/reported, ensuring that effective working partnerships are maintained and that victims of inappropriate behaviours are supported.	
Trust Health & Safety Committee	The Trust Health & Safety Committee will provide a reporting structure for the LSMS and will review submitted reports that incorporate actions taken under this policy, providing oversight and assurance that appropriate actions are being taken.	

5 Development and Consultation process

Consultation summary		
Date policy issued for consultation	7th December 2020	
Number of versions produced for consultation	1	
Committees / meetings where policy formally discussed	**Date(s)**	
Trust Health & Safety Committee		
Trust Policy Management Development Group	28th January 2021	
Where received	**Summary of feedback**	**Actions / Response**
Policy Development Group		
Trust Executive	Error with Exec Lead identified Para 3.1.1 use of term identified requirement in relation to security	Amendments made to reflect feedback.

Trust Wide Consultation	Para 3.1.1 Contracted Security Officer duties Setting of building Alarm Systems Use of full names on name badges Loss of personal issue safety alarms	Amendments made to reflect feedback.
Health & Safety Committee membership		

*(*Add rows as necessary)*

6 Reference Documents

Risk Management Policy (RS01)
Lockdown Guidance, 2009. NHS SMS
Mobile Phone and Handheld Computing Device Policy (CG12)
Remote Working and Remote Access Policy (CG20)
Information Communication and Technology Policy (IG02)
Police Interventions Policy (RS14)
Unacceptable Behaviour Policy (CG02)
CCTV Policy (IG10)
Lone Working Policy (RS04)
Searching Of Service Users (RS45)
Incident Reporting Policy (RS02)
Department of Health, Health Building Note (HBN) 03-01: Adult Acute Mental Health Units' (2003).
Additional Guidance to National Minimum Standards for General Acute Services in Psychiatric Intensive Care Units (PICU) and Low Secure Environments' (2002).
Royal College of Psychiatrists' 'Standards for Low Secure Services' (2012).
Department of Health, Environmental Design Guide 'Adult Medium Secure Services' (2011).

7 BIBLIOGRAPHY

None

8 GLOSSARY

None

9 AUDIT AND ASSURANCE

Element to be monitored	Lead	Tool	Freq	Reporting Arrangements	Acting on Recommendations and Lead(s)	Change in Practice and Lessons to be shared
Security Risk Assessment Reports – using format detailed at Appendix 2	LSMS	Site Security Reviews	Quarterly	Trust Health & Safety Committee and Estates Risk Committee	LSMS Team Managers Estates	Via Health and Safety Committees (Trust and Local)
Follow up of security incidents and breaches	LSMS	Automated ECLIPSE Incident Reports	As reported	Trust Health & Safety Committee	LSMS Team Managers Estates	Via Health and Safety Committees (Trust and Local) to Clinical Governance Committee
Monitor and Review completed action plans to ensure recommendations are addressed	LSMS	Health & Safety Audit Spreadsheet	Quarterly	Trust Health & Safety Committee	Associate Directors of Ops CNM/CSM's Team Managers LSMS Estates	Via Health and Safety Committees (Trust and Local)
Monitoring and Compliance of Security Contracts	Estates	PFI Monitoring Processes (audit/liaison)	Quarterly	Trust Health & Safety Committee SSL/Provider Compliance Review Meetings	Associate Director of Estates & Facilities Head of PFI LSMS	Trust Health & Safety Committee SSL/Provider Compliance Review Meetings

10. APPENDICES

Appendix 1 Equality Analysis Screening Form
Appendix 2 Security Risk Assessment Template
Appendix 3 Lockdown Procedure
Appendix 4 Contraband List

Appendix 1

Equality Analysis Screening Form

A word version of this document can be found on the HR support pages on Connect
http://connect/corporate/humanresources/managementsupport/Pages/default.aspx

Title of Proposal	**Security Policy**		
Person Completing this proposal	**Stephen Laws**	**Role or title**	**LSMS**
Division	**Operations Directorate**	**Service Area**	**Acute & Urgent Care**
Date Started	**3rd December 2020**	**Date completed**	
Main purpose and aims of the proposal and how it fits in with the wider strategic aims and objectives of the organisation.			
The purpose of this policy is to provide a framework for the management of physical safety and security of premises and the assets of Birmingham and Solihull Mental Health NHS Foundation Trust.			
Who will benefit from the proposal?			
The staff, service users, visitors, and members of the public that work in, use, or visit Trust premises.			
Impacts on different Personal Protected Characteristics – *Helpful Questions:*			
Does this proposal promote equality of opportunity? *Eliminate discrimination?* *Eliminate harassment?* *Eliminate victimisation?*		*Promote good community relations?* *Promote positive attitudes towards disabled people?* *Consider more favourable treatment of disabled people?* *Promote involvement and consultation?* *Protect and promote human rights?*	
Please click in the relevant impact box or leave blank if you feel there is no particular impact.			

Personal Protected Characteristic	**No/Minimum Impact**	**Negative Impact**	**Positive Impact**	**Please list details or evidence of why there might be a positive, negative or no impact on protected characteristics.**
Age	**X**			

Including children and people over 65 Is it easy for someone of any age to find out about your service or access your proposal? Are you able to justify the legal or lawful reasons when your service excludes certain age groups				
Disability	**X**			
Including those with physical or sensory impairments, those with learning disabilities and those with mental health issues Do you currently monitor who has a disability so that you know how well your service is being used by people with a disability? Are you making reasonable adjustment to meet the needs of the staff, service users, carers and families?				
Gender	**X**			
This can include male and female or someone who has completed the gender reassignment process from one sex to another Do you have flexible working arrangements for either sex? Is it easier for either men or women to access your proposal?				
Marriage or Civil Partnerships	**X**			
People who are in a Civil Partnerships must be treated equally to married couples on a wide range of legal matters Are the documents and information provided for your service reflecting the appropriate terminology for marriage and civil partnerships?				
Pregnancy or Maternity	**X**			
This includes women having a baby and women just after they have had a baby Does your service accommodate the needs of expectant and post natal mothers both as staff and service users? Can your service treat staff and patients with dignity and respect relation in to pregnancy and maternity?				
Race or Ethnicity	**X**			
Including Gypsy or Roma people, Irish people, those of mixed heritage, asylum seekers and refugees What training does staff have to respond to the cultural needs of different ethnic groups? What arrangements are in place to communicate with people who do not have English as a first language?				
Religion or Belief	**X**			
Including humanists and non-believers Is there easy access to a prayer or quiet room to your service delivery area? When organising events – Do you take necessary steps to make sure that spiritual requirements are met?				
Sexual Orientation	**X**			
Including gay men, lesbians and bisexual people Does your service use visual images that could be people from any background or are the images mainly heterosexual couples?				

Does staff in your workplace feel comfortable about being 'out' or would office culture make them feel this might not be a good idea?				
Transgender or Gender Reassignment	**X**			
This will include people who are in the process of or in a care pathway changing from one gender to another Have you considered the possible needs of transgender staff and service users in the development of your proposal or service?				
Human Rights	**X**			
Affecting someone's right to Life, Dignity and Respect? Caring for other people or protecting them from danger? The detention of an individual inadvertently or placing someone in a humiliating situation or position?				
If a negative or disproportionate impact has been identified in any of the key areas would this difference be illegal / unlawful? I.e. Would it be discriminatory under anti-discrimination legislation. (The Equality Act 2010, Human Rights Act 1998)				
		No		
What do you consider the level of negative impact to be?	**High Impact**	**Medium Impact**	**Low Impact**	**No Impact**
If the impact could be discriminatory in law, please contact the **Equality and Diversity Lead** immediately to determine the next course of action. If the negative impact is high a Full Equality Analysis will be required. If you are unsure how to answer the above questions, or if you have assessed the impact as medium, please seek further guidance from the **Equality and Diversity Lead** before proceeding. If the proposal does not have a negative impact or the impact is considered low, reasonable or justifiable, then please complete the rest of the form below with any required redial actions, and forward to the **Equality and Diversity Lead.**				
Action Planning:				
How could you minimise or remove any negative impact identified even if this is of low significance?				

How will any impact or planned actions be monitored and reviewed?
How will you promote equal opportunity and advance equality by sharing good practice to have a positive impact other people as a result of their personal protected characteristic.
Please save and keep one copy and then send a copy with a copy of the proposal to the Senior Equality and Diversity Lead at hr.support@bsmhft.nhs.uk. The results will then be published on the Trust's website. Please ensure that any resulting actions are incorporated into Divisional or Service planning and monitored on a regular basis.

Appendix 2

Service Area		**Site/Address**	
Reference Number		**Unit/Team**	
Assessor(s)		**Date Completed**	
Service Manager		**Review Date**	

Activity	Appropriate Yes/No/n/a	Hazard and Harm	Key persons at risk	Existing Controls
External Perimeter		Unauthorised access Theft or Damage to Trust property & assets Violence & aggression	BSMHFT Employees, SU's, Visitors, Contractors, General Public	Any Damage to gates/fencing? Yes/No Any automated barriers? Yes No All entry points secured, as necessary. Yes/No CCTV coverage? Yes/No Anti-Climb Measures? Yes/No/n/a Courtyard/Garden Furniture secured and correctly positioned/ Yes/No/n/a
Inner Perimeter				
Internal Courtyards		Risk of harm Absconding Access to roof	Service Users BSMHFT Employees	

Activity	Appropriate Yes/No/n/a	Hazard and Harm	Key persons at risk	Existing Controls
Car Parks / Grounds & Internal Approach		Risks of violence & aggression Theft/damage to/from vehicles Obstruction for Emergency service access	BSMHFT Employees, SU's, Visitors, Contractors, General Public	CCTV coverage? Yes/No Footpaths clear & unobstructed? Yes/No Lighting/CCTV unobscured by trees/shrubs? Yes/No Vehicle access routes clear & unobstructed? Yes/No All vehicles parked within designated parking spaces. Yes/No Blue badge parking available & used by authorised permit holders? Yes/No
Lighting Provision		Personal safety & slips trips & falls due to poor lighting provision.	BSMHFT Employees, SU's, Visitors, Contractors, General Public	Any visible damage to lighting? Yes/No Access/egress points well lit? Yes/No All external lighting operational? Yes/No. Lighting provision unobscured by trees/shrubs? Yes/No
Building Shell			BSMHFT Employees, SU's, Visitors, Contractors, General Public	Building in good state of repair? Yes/No Privacy film to publicly facing external windows. Yes/No Any visible damage to building? Yes/No Visible Alarm Sounder Boxes? Yes/No n/a
Main Entrance				CCTV coverage of areas? Yes/No Access Control Mechanism? Yes/No Doors Closing fully and securing? Yes/No
Dedicated Staff Entrance				
Secure/ Out of Hours Entrance				

Activity	Appropriate Yes/No/n/a	Hazard and Harm	Key persons at risk	Existing Controls
Reception Desk			BSMHFT Employees, SU's, Visitors, Contractors, General Public	Security Screen Yes/No Visitors Greeted Yes/No *Sign in/Visitors Book Yes/No *Identification checked Yes/No Staff clearly identifiable & name badges worn. Yes/No CCTV coverage of area? Yes/No "refer to additional checks at end of document.
Waiting Areas		Physical & Verbal assault Damage to property	BSMHFT Employees, SU's, Visitors, Contractors, General Public	Appropriately Furnished? Yes/No CCTV coverage of area? Yes/No Have all items that could be used as a weapon been removed or action taken to secure them? Yes/No
Building Access Control/ Locking		Unauthorised access Physical/Verbal assault Theft Damage Breach of confidentiality	BSMHFT Employees, SU's, Visitors, Contractors, General Public	Access Control system used? Yes/No (details). Are all doors secure/locked that should be? Yes/No Process in place for key/access card management? Yes/No Staff aware how to report loss/theft of keys/access cards? Yes/No Controls in place for changing access codes to doors. Yes/No Procedure for securing the building out of hours. Yes/No n/a
Control of Visitors		Unauthorised access Physical/Verbal assault Theft	BSMHFT Employees, SU's, Visitors, Contractors	Visitors escorted to and from waiting areas by staff? Yes/No

Activity	Appropriate Yes/No/n/a	Hazard and Harm	Key persons at risk	Existing Controls
		Damage Breach of confidentiality		
Consultation Rooms / Publicly accessible rooms		Physical or verbal abuse Potential Hostage incidents Risk of individuals locking themselves in rooms Self-Harm	BSMHFT Employees, SU's, Visitors, Contractors, General Public	Appropriately furnished? Yes/No Anti-Barricade Measures fitted? Yes/No Door Vision Panels fitted? Yes/No Have all items that could be used as a weapon been removed or action taken to secure them? Yes/No Door can be locked from the inside. Yes/No. If Thumb turns present, are these clutched mechanisms? Yes/No n/a
Anti – Barricade Measures		Potential Hostage incidents Risk of individuals locking themselves in rooms Self-Harm	BSMHFT Employees, SU's, Visitors, Contractors, General Public	Anti-Barricade measures fitted to all rooms publicly accessible? Yes/No Staff trained & aware how to use anti-barricade measures? Yes/No N/A
"Blind Spot" Zones		Risks to individuals due to areas within buildings without natural line of observation.	BSMHFT Employees, SU's, Visitors, Contractors, General Public	Security Mirrors installed? Yes/No Security mirrors required to mitigate risks of "blind spots" within circulation routes? Yes/No
Staff Assistance Alarm Systems		Staff unable to summon assistance in emergency	BSMHFT Employees, SU's, Visitors, Contractors,	Alarm activation panels appropriate & sufficient? Yes/No Sufficient fobs/receiver units providing required cover? Yes/No

Activity	Appropriate Yes/No/n/a	Hazard and Harm	Key persons at risk	Existing Controls
			General Public	Clear and understood response protocol? Yes/No Response protocol tested. Yes/No Alarm system/fobs testing process in place and document? Yes/No / NA Staff aware how to report faults with fobs? Yes/No Documented process for allocation and return of alarm fobs? Yes/No
Key Management		Unauthorised access Loss/theft of controlled keys/access cards	BSMHFT Employees, SU's, Visitors, Contractors,	Documented process for allocation & return of keys/access cards? Yes/No All keys/access cards held securely when not allocated? Yes/No Staff understand how to report lost/missing keys/access cards? Yes/No
Handling Money/ Valuables			BSMHFT Employees, SU's, Visitors, Contractors, General Public	Cash storage on site? Yes/No Safe provided? Yes/No Cash handling restricted to authorised staff. Yes/No If cash transferred between sites, a process is in place to ensure activity is varied? Yes/No N/A Procedures & policy in place for storage of service user property? Yes/No N/A
Security of Drugs, Medicines and Treatment rooms			BSMHFT Employees, SU's, Visitors, Contractors,	Door kept secure when not in use? Yes/No Privacy film to any external facing windows? Yes/No Blinds fitted and kept closed Prescription pads stored securely. Yes/No N/A

Activity	Appropriate Yes/No/n/a	Hazard and Harm	Key persons at risk	Existing Controls
				Drug/Medicine cabinets secured and access restricted? Yes/No Anti-Barricade Measures fitted to door? Yes/No
Violence Aggression/assault		Physical or verbal assault by SUs	BSMHFT Employees, SU's, Visitors, Contractors, General Public	Are staff aware of procedure to follow when actual or potential incident occurs? Yes/No If staff assistance alarm sounds do staff know what to do? Yes/No Are staff aware of support available re incidents of V&A? Yes/No Do staff know how to report incidents? Yes/No
Lone Working / Isolated Working		Physical or verbal abuse, injury	BSMHFT Employees, SU's, Visitors, Contractors, General Public	Are local lone working processes and procedures in place? Yes/No N/A Is there a process for staff to report any out of hours working? Yes/No N/A Are staff issued with and use the Trust Lone Working Solution? Yes/No N/A Are escalation processes in place to alert staff to risks of V&A from SU's or relatives/associates at their address? Yes/No Where significant risks identified, can services be provided within a Trust building to help mitigate these risks to community workers? Yes/No N/A Is lone or isolated working within a building essential? Yes/No
Intruder Alarms			BSMHFT Employees,	Alarm Sounder box visible? Yes/No

Activity	Appropriate Yes/No/n/a	Hazard and Harm	Key persons at risk	Existing Controls
			SU's, Visitors, Contractors, General Public	Who activates/deactivates the alarm system? Process in place for staff to secure building.
CCTV **External CCTV**			BSMHFT Employees, SU's, Visitors, Contractors, General Public	Are All Cameras operational? Yes/No Is system compliant with Trust Policy? Yes/No Is recording equipment kept in secure location? Yes/No CCTV monitors situated appropriately. Yes/No Are local staff trained to operate basic functions of the system? Yes/No N/A Time & date stamp of system correct. Yes/No CCTV Warning signs prominently displayed? Yes/No
Internal CCTV				
Site Security			BSMHFT Employees, SU's, Visitors, Contractors, General Public	Security Checks in place at main entrance? Yes/No Site patrols conducted. Yes/No Escort service available for staff. Yes/No
Outbuildings			BSMHFT Employees, SU's, Visitors, Contractors, General Public	All outbuildings secure/locked? Yes/No Any visible damage to outbuildings? Yes/No CCTV coverage? Yes/No Any materials/operational equipment stored insecurely? Yes/No

Activity	Appropriate Yes/No/n/a	Hazard and Harm	Key persons at risk	Existing Controls
External Waste storage		Arson Damage to buildings & property	BSMHFT Employees, SU's, Visitors, Contractors, General Public	Site has dedicated secure waste storage area. Yes/No Waste storage area locked to prevent unauthorised access. Yes/No Where no dedicated storage, are bins secured to prevent security risks to site? Yes/No N/A Discarded/damaged equipment stored securely? Yes/No CCTV coverage? Yes/No
Medical gases		Theft	BSMHFT Employees, SU's, Visitors, Contractors, General Public	Dedicated secure storages area? Yes/No Alarm system fitted. Yes/No N/A CCTV coverage? Yes/No N/A

Security – ID Checks Ask 5 people not wearing identification within staff/secure areas if you can see their ID Card								
	Employees based on site	**Employees not based on site**	**Visitor**	**Contractor or Other**	ID Displayed	ID Carried	No ID displayed or carried	If visitor/contractor check log
1								
2								
3								
4								
5								
Additional Information								
Record the last 5 entries in the visitors' book (date & time) if in use.								
	DATE		**TIME**	**COMMENTS**				
1								
2								
3								

4			
5			
Additional Information			

KEY FINDINGS & COMMENTS RECEIVED

RECOMMENDATIONS & ACTION PLAN

Risk Assessment Action Required	Clinical Area Lead Responsible for Action	Estates/ Facilities Lead Responsible for Action	Estates Work Order Number	Health & Safety Lead Responsible for Action	Risk Rating (example)	Agreed Date Required to be Completed by (RAG Rating)	Date Action Completed
					High		
					Medium		
					Low		

Appendix 3

Lockdown Procedure – General Guidance

1. Introduction

It is essential that the Trust is able to respond appropriately to a variety of threats and hazards. It is therefore necessary to have a clear and comprehensive procedure for the implementation of lockdown so that staff, services users, visitors and property are protected as fully as possible.

This Lockdown Procedure aims to provide guidance regarding the types of incidents that may result in Lockdown and how this should be activated.

2. Purpose

This procedure has been developed in order to set out the Trust's general arrangements for implementing a lockdown. It takes into account the requirements of NHS Protects' guidance eon Lockdown, Civil Contingencies, the Public Health Act and the Human Rights Act. This procedure applies to all Trust sites and premises.

3. Definitions

A Lockdown is the process of controlling the movement, access and egress of people (staff, patients and visitors) around Trust sites or premises in response to an identified risk, threat or hazard that might impact upon the security of staff, service users and assets or the capacity of that site/premises to operate.

There are four stages to Lockdown. These are:

1. Activation
2. Deployment
3. Maintenance
4. Stand-down

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

Lockdown does not prevent people from escaping from a hazard such as fire or flood, but is to secure the building once evacuation has taken place or to prevent access to areas that may pose a risk. Lockdown can be full, progressive or partial.

The overarching aim of implementing a lockdown is to either **exclude** or **contain** staff, service users and visitors.

Supporting the overarching objective of excluding or containing staff, patients or visitors, a lockdown may be characterised as a **partial (static or portable), progressive** or **full** lockdown.

A **partial lockdown** can be defined in a number of ways. In most instances, a partial lockdown is the locking down of a specific part of the Trust or a specific building or part of a building. A partial lockdown is also when entry restrictions are placed on a specific building to control the flow of people into it – via identification checks for example. This is also known as 'controlled access' to a site or building. On these occasions, the partial lockdown can also be characterised as being 'static'

A **progressive lockdown**, which can also be called an **incremental lockdown**, can be a step-by-step lockdown of a trust site or building in response to an escalating scenario. For instance, a trust locks down its A&E department based on specific intelligence – for example, a white powder incident. As time progresses and with additional intelligence, the decision to lock down other departments is taken because of the fear of contamination. In this situation, a trust should be able to systematically expand its lockdown across its various departments. This lockdown will be implemented in a fairly ordered manner

A **full lockdown** is the process of preventing freedom of entry to and exit from either the entire Trust or from a specific building.

4. Duties

Role	Duties, Responsibilities and Accountabilities
The Chief Executive and/or Director of Operations.	The Chief Executive and/or the Director of Operations have the default authority to call a Lockdown situation.
On Call Associate Director/ Senior Manager	In accordance with Major Incident Protocols, authority to call a Lockdown is delegated to the On Call Director/Senior Manager. However, there may be occasions when a manager present at an incident location calls for a Lockdown following a dynamic assessment of the situation. In such an event, the On Call Director/Senior Manager, must be notified immediately after the Lockdown has been called.
Ward/Unit/ Team Managers	Managers must seek the approval from the On Call Director/Senior Manager of any incident they believe may justify a Lockdown. However, circumstances may be such that a dynamic risk assessment of the situation calls for an immediate Lockdown, in which case the Manager has the delegated authority to do so. The On Call Director/Senior Manager must be immediately informed.
All Staff	Staff must be aware of local emergency procedures. In the event of a Lockdown or major incident, staff must follow directions from the incident lead.

4. Activation of Lockdown

The decision to activate a Lockdown should be based on:

- The potential for harm to people or property
- Whether it is possible to isolate or neutralise the source of the threat or hazard
- How far people or property are from the source of the threat or hazard
- Possibility of cross contamination

The scenario's that may warrant the activation of a lockdown and may also be categorised as a Major Incident are:

- Fire
- Baby or Child Abduction from Mother & Baby Unit at the Barberry
- Acts of Terrorism
- Hostage Situations
- Chemical, Biological contamination (including self-presenting individuals and "worried well" inappropriately attending BSMHFT Sites
- Structure Collapse
- Escape of a Patient from Medium Secure Unit.
- Loss or theft of keys from Medium Secure Unit.

Lockdown scenarios are categorised in 3 levels:

Level 1 – Full lockdown the whole building, foot and road accesses.
Level 2 – Specific building or buildings on sites with multiple units.
Level 3 – A specific department.

The matrix below indicates the level of lockdown against a particular scenario and the type of lockdown to be implemented depending on the scale of the incident.

SCENARIO	LEVEL 1	LEVEL 2	LEVEL 3
Fire		**Progressive**	**Progressive**
Baby abduction	**Containment**		
Acts of terrorism		**Full**	**Full**
Hostage situation		**Partial**	**Partial**
Chemical or biological contaminations		**Partial**	**Partial**
Structure collapse		**Full**	**Full**
Utilities explosion		**Full**	**Full**
Loss of Theft of MSU keys		**Full**	**Full**
Escape of Patient from MSU	**Full**		

Because the Trust's buildings are usually open to the public, members of the public have an implied licence to enter them. However, the owner of any such premises has

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

If a casualty or a patient attends a locked down healthcare site or building, the doctrine of best interest may be applicable. In this instance, although the casualty or patient requires treatment, it will be in their best interest to receive that treatment at other, safer, healthcare premises. Consequently, their 'right to treatment' under the Human Rights Act 1998 will not be infringed upon.

In the absence of the police, who are able to enforce a containment cordon, it will only be lawful for an NHS trust to prevent the **exit** of a significant number of people from its premises by utilising specific legislative provision (e.g. emergency regulations under the Civil Contingencies Act and/or Public Health Control of Disease Act 1984) which provides for the protection of the public from notifiable diseases. Even when these specific regulations can be used, specific tenets of the Human Rights Act 1998 must also be considered – for example, a person's right to liberty (Article 5) and an individual's right to a family (Article 12). Without these regulations, exit could **only** be prevented in relation to specific individuals in certain circumstances, limited to the following situations:

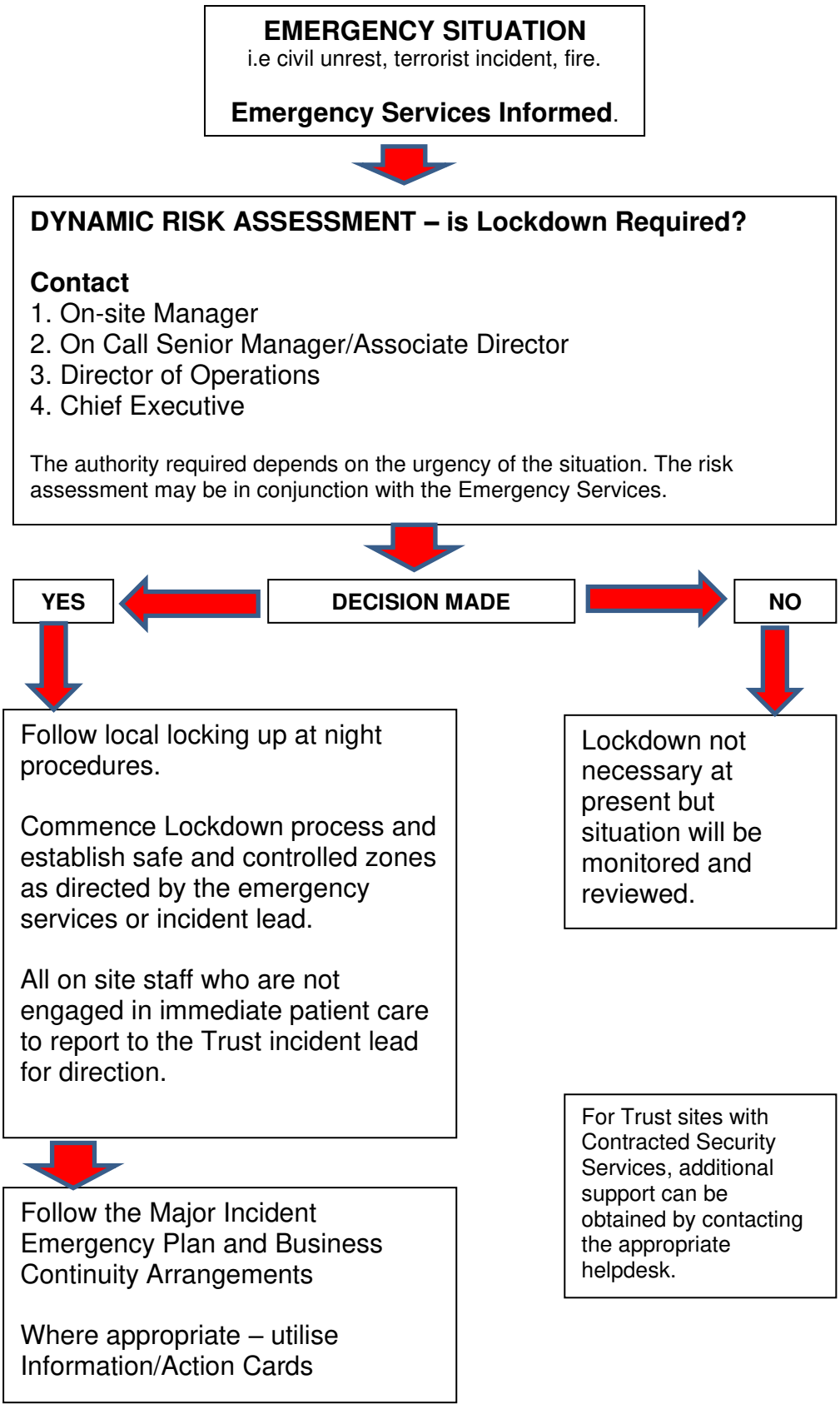
- The individual is committing an offence or causing injury or damage to property which may lead to them being arrested

- They are detained under the Mental Health Act or otherwise lawfully detained.

While NHS professionals can give direction within their premises (for example, stating which exit someone can use), it is unlawful to forcibly prevent exit from NHS premises unless it is for the reasons stated above. Without these justifications, NHS staff could be open to legal action under the criminal and/or civil law if they prevented a person from leaving.

Nonetheless, there may be circumstances when a lockdown which prevents individuals from exiting NHS premises (or part of them) are desirable. If this occurs, NHS staff can only appeal to individuals to stay in the site and/or building identified for lockdown. If individuals choose to exit, a safe route must be available for them to do so.

FLOWCHART FOR LOCKDOWN PROCEDURE



Appendix 4

Contraband items

All mental health inpatient services have some prohibited or 'contraband' items. The following are typically banned in all inpatient services:

- Alcohol and drugs or substances not prescribed (including illicit and legal highs)
- Items used as weapons (firearms- real or replica, corrosive liquids, 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
- Equipment that can record moving or still images (camera, web cameras)

Whilst a least restrictive approach is encouraged in relation to the restrictive use of IT items, and such restrictions must be commensurate with the security requirements of the service/building, secure mental health units may also prohibit:

- Mobile phones (though may be allowed in some rehabilitation low secure units)
- Computers, tablets, games devices with hard drives or sharing capabilities
- Items with voice recording capabilities
- Other items with enabled WiFi/internet capabilities
- Items considered as an escape aid

Restricted items

Restricted items are items to which 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
- Identity documents, bank cards, items of stationery
- Cutlery, tinned materials, glassware