

Security Policy (including The Prevention and Control of Violence & Aggression)

CATEGORY:	Policy
CLASSIFICATION:	Governance
PURPOSE	To set out the principles and framework for the management of Security within the Trust, to ensure that all staff understand their roles and responsibilities.
Controlled Document Number:	146
Version Number:	7.0
Controlled Document Sponsor:	Chief Legal Officer
Controlled Document Lead:	Trust Security Management Specialists
Approved By:	Board of Directors
On:	28/10/2020
Review Date:	28/10/2023
Distribution:	All Trust Staff
• Essential Reading for:	
• Information for:	

Contents

Paragraph		Page
1	Policy Statement	3
2	Scope	3
3	Framework	3
4	Duties	8
5	Implementation	12
6	Monitoring	13
7	References	13
8	Associated Policy and Procedural Documentation	13
Appendices		
Appendix A	Monitoring Matrix	15

1 Policy Statement

- 1.1 The Trust is committed to providing a safe and secure environment for all patients including children and young persons, visitors, staff and all workers engaged within the Trust. In particular, the Trust will not tolerate harassment, violence and/or aggression without lawful justification or excuse.
- 1.2 The objective of this policy is to ensure that the Trust provides a secure and safe environment which minimises security risks to all patients, staff and visitors alike and also protects the property, assets, service delivery and the reputation of the Trust so that:
 - 1.2.1 There is a safe and secure environment with regards to persons, functionality and physical assets;
 - 1.2.2 There is a unified, structured and proactive approach to the management of security and violence and aggression within the Trust with all due consideration of legislative, regulatory and mandatory obligations; and
 - 1.2.3 All persons are aware of their roles, responsibilities and obligations with regards to security matters

2 Scope

For the purposes of security this policy applies to all Trust staff, including Contractors, UHB+ staff, staff on Honorary Contracts, Agency, and Locum workers as well as those undertaking secondments whether they are involved in Trust business whilst on any property owned or controlled by the Trust or off Trust premises. Nominated managers must therefore ensure that any non-employed workers are aware of the requirements of this policy and the associated procedures and how to apply them.

3 Framework

- 3.1 This section describes the broad framework for the Security Policy. Detailed instructions are provided in the associated procedural documents.
- 3.2 The Chief Legal Officer shall approve all procedural documents associated with this policy, and any amendments to such documents, and is responsible for ensuring that such documents are compliant with this policy.
- 3.3 **Security – General**

This policy should be read in conjunction with the security procedure. Contracted Security refers to the two organisations which provide a security service across the Trust on a site specific basis.

In order to achieve a safe and secure environment for all, the Trust shall:

- 3.3.1 Ensure that risks are properly identified, assessed, and that appropriate mitigation measures are put into place (“Security Risk Assessments”) in accordance with the Security Procedure;
- 3.3.2 Make available appropriate resources to implement this policy effectively. The Trust’s security service for the main sites is provided by a contracted service that has a dedicated security manager with overall responsibility for security staff, the security contract will be overseen by the relevant Trust Security Management Specialist. (TSMS)
- 3.3.3 Clearly set out the responsibilities of staff at all levels;
- 3.3.4 Provide guidance on how to manage security issues and incidents;
- 3.3.5 Monitor the effectiveness of such measures taken and to make any necessary amendments to policies and procedures;
- 3.3.6 Provide suitable support, advice and guidance to those involved and exposed to security incidents; and
- 3.3.7 Sustain positive relationships with other key stakeholders e.g. law enforcement organisations, neighbours, the National Counter Fraud and Security Management Service, the Health and Safety Executive and other regulatory bodies.

3.4 **Management of Violence and Aggression**

Within the context of this policy the following definitions, taken from NHS Protect guidance and Health and Safety Executive (HSE) are used:

- 3.4.1 Assault is described as ‘the intentional application of force against the person of another without lawful justification, resulting in physical injury or personal discomfort’; and
- 3.4.2 Verbal aggression is ‘the use of inappropriate words or behaviour causing distress and/or constituting harassment’.

HSE Definition. Any incident in which a person is abused, threatened or assaulted in circumstances relating to their work.

For all incidents of violence and aggression the Trust will ensure, where appropriate, that:

- 3.4.3 potential triggers to violence and aggression are risk assessed as part of the security risk assessments by Nominated Managers;

- 3.4.4 reasonable measures to reduce the likelihood of violence and aggression are devised and implemented to address specific risks by Nominated managers and the security teams (as appropriate);
- 3.4.5 consideration is given to excluding patients/public who present an unacceptable risk in accordance with the Withholding Treatment Procedure;
- 3.4.6 specialist advice on appropriate control mechanisms will be provided by the Trust Security Management Specialist.
- 3.4.7 support is provided to any member of staff involved in an incident of violence or aggression;
- 3.5 Where staff are either violent and/or verbally aggressive to any persons the Trust's Disciplinary Procedure will be followed.
- 3.6 Where a patient is subject to violence and or verbal aggression from another patient and or a member of the public and it appears that there is a safeguarding risk the Trust's Safeguarding Processes shall be adhered to.
- 3.7 All incidents of violence and aggression must be recorded on the Trust Incident reporting system, the initial incident will be managed by Trust staff and the Contracted Security service who will attend the incident if requested to do so. Police should also be informed should a criminal offence be committed, the incident will be overseen by the Trust Security Management Specialist for that Hospital. The TSMS team will support staff with consideration of pursuing criminal compliant.
- 3.8 The instructions provided in the associated Security Procedure must be followed.
- 3.9 **Major Incidents and Serious Threats**
 - 3.9.1 The Trust Major Incident Plan will be implemented in the event of a major security incident. In such circumstances, this plan will supersede or enhance the security measures outlined within this policy and the Emergency Preparedness Policy
 - 3.9.2 Serious threats, including terrorist threats, to the Trust will be assessed and appropriate measures will be implemented commensurate with the nature and level of risk.
 - 3.9.3 The implementation of general preventative measures will reflect the five national levels of threat, ranging from low (i.e. unlikely attack) to critical (i.e. expected imminent attack) and will include an increase in

the frequency of the Contracted Security's preventative patrols in the event of a rise in the national threat level.

3.9.4 If the Trust is advised by West Midlands Police Counter Terrorism Security Advisors of a specific terrorist threat or other serious threat to the Trust or health bodies generally, the Trust Security Management Specialist will inform the Executive Team and where appropriate, Contracted Security and they will assess the individual risk and put in place measures to counteract the risk.

3.10 **Lock-down**

A Lock Down enables an entire building/site or parts of the building/site to be locked down in the event of a serious incident. The TSMS shall, in conjunction with Contracted Security where appropriate, ensure that a lock down procedure is in place. The Trust's Lock Down Procedure provides full details around the implementation of the lock down for each site.

3.11 **Management of Security Incidents**

3.11.1 All Trust **staff** will report any security incidents to contracted security and also report details of the incident on the Trust incident reporting system. The Contracted Security will respond to all security incidents in accordance with the contractual requirements placed upon them. The TSMS shall monitor this response and management of any incident to ensure that it is appropriate given the circumstances of the incident. Where appropriate TSMS will co-ordinate/lead a response.

3.11.2 All security incidents attended by contracted security will be documented, and TSMS will be informed, using Datix or other agreed reporting systems, in the event of a Major Incident escalation procedures must be followed.

3.12 **Security of Trust Assets**

3.12.1 All Nominated Managers are responsible for the safety and security of all Trust assets within their area of responsibility. This responsibility includes carrying out a local risk assessment and putting in place suitable security measures for when the equipment is in storage.

3.12.2 Trust Property must not be removed from its intended point of use or safe storage without permission from a suitably authorised person.

3.12.3 All materials and equipment must be used, stored and maintained in accordance with their intended purpose and manufacturer's recommended instructions.

3.13 The following matters are dealt with in the Security procedure.

- **Identification Badges and Access Control Cards:** All Trust staff must display Trust issued identity badges at all times when on duty.
- **Key Management**
- **Termination of Employment**

3.14 **Lone Working**

Nominated Managers shall be responsible for identifying any staff who are subject to lone working or staff who suspect they will be lone working must inform their nominated manager who will complete a risk assessment. They will develop and agree suitable working practices, in accordance with the Trust Lone Worker procedure including the consideration to the issue of an approved lone worker alarm.

3.15 **Security of Information**

This is covered in the Data Protection and Confidentiality Policy.

3.16 **Security of Trust Vehicles**

This is covered in the Motor Vehicle Policy

3.17 **Car Parking**

3.17.1 All vehicles parked on Trust property shall be at the owner's risk and the Trust will not be held liable for any damage, however caused.

3.17.2 All drivers are required to abide by the terms and conditions that are contained within the Trust's Traffic Management Policy

3.18 **Waste and Hazardous Items**

All waste including potentially hazardous items must be segregated, handled, contained, secured and stored in accordance with the Trust's Waste Policy and its associated procedure.

3.19 **Training**

The Trust will ensure that Conflict Resolution and other appropriate training, is provided in accordance with the Trust's Training Catalogue (Training Needs Analysis).

3.20 **Trust Health, Safety and Environment Committee**

The Trust Health Safety and Environment Committee regularly assesses and reviews security activity, trends, risks and issues across the Organisation as a whole. The Committee recommends the development of action plans by the TSMS with a view to mitigating or eradicating such risks. The Chair of the Committee reports to the Trust Board.

4 Duties

4.1 Chief Legal Officer

4.1.1 In accordance with the requirements of the Secretary of State Directions for Health, The Chief Legal Officer has been appointed as the Trust's Security Management Director in accordance with Directions to NHS Bodies on Security Management Measures 2004 . The post holder shall act on behalf of the Board of Directors as the named Director with overall responsibility for Security Management arrangements within the Trust.

4.1.2 They shall provide assurance to the Board of Directors on compliance with this policy and report any material failures of compliance or other security concerns including violence and aggression.

4.2 Director for Corporate Affairs.

The Director for Corporate Affairs shall have responsibility for the planning and delivery of security management arrangements and provide cover in the absence of the Security Management Director.

4.3 Trust Security Management Specialists

The Trust's Security Management Specialists (TSMS) will be responsible for co-ordinating and delivering a professional operational security management service. In so doing, the post holder shall:

4.3.1 Ensure that contracted security comply with the contractual requirements, and escalate any potential or actual contract breaches to contract manager.

4.3.2 Ensure contracted security carry out any contractual requirements around the completion of the perimeter security risk assessments;

4.3.3 Provide specialist support, advice and assistance in relation to all security and violence and aggression matters;

4.3.4 Develop and implement appropriate Trust-wide security policies and procedures;

4.3.5 Support the development of localised operational security procedures within all areas of the Trust;

4.3.6 Act as the main point of contact with the National Counter Fraud law enforcement agencies and other such organisations;

- 4.3.7 Monitor security equipment to ensure that it is functional and appropriately maintained;
- 4.3.8 Liaise with the Police where necessary and to provide information on identified perpetrators of violence and other crime;
- 4.3.9 Collate and analyse reported security incidents, identifying trends in the interventions required of security staff in respect to all security incidents including violent incidents; and report findings in a Quarterly Health and Safety Report.

4.4 Senior Divisional and Corporate Directors/Managers (Including Directors of Operations and Associate Directors of Nursing)

Senior Divisional and Corporate Directors/Managers will be responsible for ensuring that this policy and associated practices, as well as local security procedures are implemented and effectively managed within each of their areas of responsibility. They will ensure that each department under their control undertake a security risk assessment, including the potential for violence and aggression, implement controls where risks are identified and monitor these for effectiveness.

4.5 Heads of Departments, Group Managers and Matrons and Nominated Managers

All Heads of Departments, Group Managers and Matrons and Nominated Managers are responsible for:

- 4.5.1 ensuring local security procedures are in place;
- 4.5.2 undertaking a comprehensive departmental risk assessment and creating an environment and climate where violence is less likely;
- 4.5.3 ensuring that the Policy, the associated Procedures, guidelines and are made known and available to all their staff;
- 4.5.4 supporting any member of staff who has been involved in any security incident including violence and aggression;
- 4.5.5 ensuring that an online Incident Report Form is completed for every security incident including violence and/or aggression.
- 4.5.6 Prevention, control measures and monitoring arrangements are implemented once identified in local security risk assessment's;
- 4.5.7 All staff are made aware of their obligations and receive appropriate advice, education and required training.

4.6 Ward/Departmental Managers and Supervisors

Ward/Departmental Managers and Supervisors will be responsible for ensuring that Security policies, practices and procedures are complied with, which shall include:

- 4.6.1 Ensuring that local security procedures are adhered to and that all actual or potential breaches, acts of assault, violence or aggression are reported using the Trust incident reporting system and action plans devised as required;
- 4.6.2 Ensuring that all security equipment is fully functional and reporting any faults to relevant department for prompt repair.
- 4.6.3 Ensuring that Trust assets, property and information are not left unattended and are correctly and securely stored at all times;
- 4.6.4 Ensuring that the department is kept secure and locked when unattended;
- 4.6.5 Ensure that all patients are made aware of the risks associated with bringing in large amounts of money or valuables into the Trust and where this responsibility is delegated to staff that the patient property policy and procedures are followed.

4.7 **All staff**

All staff are responsible for assisting and supporting in the provision of a secure and safe environment and to this aim they must:

- 4.7.1 Ensure all staff know how to contact the contracted security service for the location the incident, and ensure all staff follow this policy and associated procedures, including local security arrangements;
- 4.7.2 Maintain a high degree of vigilance and not undertake any actions that may compromise their own personal safety, or that of colleagues, patients or visitors;
- 4.7.3 Report any security risks and concerns to their Line Manager;
- 4.7.4 Attend relevant security training and awareness sessions;
- 4.7.5 Report any malfunctioning of security equipment at the earliest possible opportunity.
- 4.7.6 Not interfere with or misuse any security equipment, property or the environment as a whole;
- 4.7.7 Ensure that they wear Trust ID badge, in a visible position at all times;

- 4.7.8 Challenge any persons not known to them and not wearing an authorised Trust ID badge;
 - 4.7.9 Ensure that Trust assets are not removed from their intended location without appropriate authorisation;
 - 4.7.10 Ensure that their personal property is kept secure at all times;
 - 4.7.11 Try to de-fuse violent/aggressive situations if they feel safe to do so and immediately summon assistance when aware of a potential or actual violent incident;
 - 4.7.12 If involved in an incident either as a victim or when going to someone's assistance, use the minimum of force necessary to control the violent person(s) bearing in mind the legal/medical constraints and personal responsibility to act within the law; and
 - 4.7.13 Complete an online Datix Incident Report Form immediately following such an event or as soon as possible thereafter.
- 4.8 Compliance with this policy and associated procedures is mandatory and failure by any member of staff to comply with such requirements will result in consideration of the use of disciplinary action.

4.9 **Contracted Security**

Contracted Security will ensure that

- 4.9.1 An annual site security risk assessments are completed in accordance with the their contract with the Trust;
- 4.9.2 A secure, robust and fully auditable system is in place for the management and distribution of keys used by security, including master sets;
- 4.9.3 Undertake lock and unlock procedures for designated Trust premises. This includes promptly attending and assessing premises where a breach of security has been reported;
- 4.9.4 A method statement outlining security service provision is produced annually;
- 4.9.5 Ensure that all security equipment used by contracted security is fully functional and report any faults to appropriate departments to ensure a timely repair.
- 4.9.6 Respond and assist with potential and actual security incidents, including acts of assault, violence and aggression;

4.9.7 Provide continuous surveillance of security monitoring systems and undertake regular patrols (as defined within method statements) of Trust premises and grounds with a view to identifying potential risks and resolving any actual breaches of security; and

4.9.8 Investigate any breaches of security and report the finding to the Trust Security Management Specialist (TSMS).

5 Implementation and Monitoring

5.1 Implementation

5.1.1 This policy will be implemented by all levels of management in the Trust and made available to all staff via the Trust intranet.

5.1.2 In addition, information on security issues will be provided to wards and departments by the TSMS to encourage a pro-security culture among staff.

5.1.3 The TSMS will provide advice, assistance and support on various security related matters.

5.2 Monitoring

Appendix A includes full details on how this policy will be monitored by the Trust.

6 References

Secretary of State's Directions for Violence & Aggression and Security Management (2003/2004).

Health and Safety at work Act 1974

The Management of Health and Safety at Work Regulations 1999

Corporate Manslaughter and Corporate Homicide Act 2007

Civil Contingencies Act 2004

NHS Resolution

The Management of Health and Safety at Work Regulations Working Alone in Safety (HSE) Publication

Data Protection Act 2018

7 Associated Policy and Procedural Documentation

Withholding Treatment Procedure for Aggressive Patients

Lone Worker Guidelines

Security Procedure

Disciplinary Procedure

Data Protection and Confidentiality Policy

Traffic Management Policy

Major Incident Plan

Lock Down Procedure.

Waste Policy

Mandatory Training Policy.

MONITORING OF IMPLEMENTATION	MONITORING LEAD	REPORTED TO PERSON/GROUP	MONITORING PROCESS	MONITORING FREQUENCY
There is a safe and secure environment with regards to persons, functionality and physical assets: Appropriate Risk Assessments have been completed				
Departments (Nominated Managers) have completed their risk assessments (including violence and aggression and lone workers, and assets) and have local security procedures in place	TSMS	Health, Safety and Environment Committee	An Annual Audit of Risk assessments received is completed and a report identifying trends is produced	Annually
Contracted security has completed security risk assessments of premises	TSMS	Health, Safety and Environment Committee	The annual risk assessments are reported and challenge/feedback is provided.	
There is a unified, structured and proactive approach to the management of security and violence and aggression within the Trust with all due consideration of legislative, regulatory and mandatory obligations				
The security service provided by Contracted Security is monitored and issues are escalated	TSMS	Director of Corporate Affairs PFI Performance Manager	HGS: Contract related issues are raised with the Director of Corporate Affairs and escalated to the Chief Legal Officer where appropriate. At QE matters are raised with the PFI Performance Manager and escalated to the Chief Legal Officer where appropriate	Ad hoc
Trust security incidents are reviewed: security activity, trends, risks and issues across the Trust	TSMS	Trust Health, Safety and Environment Committee	The Trust Health, Safety and Environment Committee assess and reviews security activity, trends, risks and issues across the Trust every quarter.	Quarterly
Nominated Managers are aware of their roles, responsibilities and obligations with regards to security matters				
Nominated Managers are trained	Health and Safety Lead	Trust Health, Safety and Environment Committee	Health and Safety provide training for Nominated Managers and security is included. Any specific issues are signposted to the TSMS who provided 1:1 support.	Quarterly