Avon and Wiltshire Mental Health Partnership NHS Trust

Security Policy

Board library reference	Document author	Assured by	Review cycle
P040	Local Security Management Specialist	Quality and Standards Committee	3 years

This document is version controlled. The master copy is on Ourspace.

Once printed, this document could become out of date.

Check Ourspace for the latest version.

Contents

1. Introduction

Avon & Wiltshire Mental Health Partnership NHS Trust henceforth within this document referred to as the "Trust" is committed to providing a safe and secure environment for its staff, patients, carers and visitors and to maintaining the security of its premises and assets.

The provision of a safe and secure environment in this policy is recognised by the Trust as a statutory requirement.

This policy will be applied to the fair treatment of all people, regardless of their gender, race, colour, ethnicity, ethnic or national origin, citizenship, religion, disability, mental health needs, age, domestic circumstances, social class, sexuality, beliefs, political allegiance or trades union membership. The Trust is firmly opposed to any discrimination based on these human characteristics and values

2. Purpose or Aim

It is the intention of this policy and associated policies to deliver an environment, for those who use and those who work in the Trust, that is properly secure so that the highest possible standards of clinical care can be made available for service users. In particular efforts will be focussed on ensuring: the protection of all staff, service users, carers and visitors, specifically minimising and preventing violence against those providing services; and the protection of Trust Property and assets, both financial and non-financial. It also aims to:

- Protect the safety, security and welfare of staff, service users, carers, agency staff contractors and the general public, whilst on Trust property;
- Provide safe systems and safeguards against crime, loss, damage or theft of property, equipment or other assets;
- Minimise disruption or loss of service to service users and to the Trust's core activity;
- Address any security malpractices that impinge on the management of the Trust.

3. Policy Statement

The Trust believes that all staff, service users, carers and visitors should treat each other with dignity and respect and to behave in an acceptable and appropriate manner as set down in the Dignity at Work Policy. Staff have a right to work, as service users have a right to be treated, free from fear of assault and abuse in an environment that is properly safe and secure.

The Trust will ensure that systems are in place to provide a safe and secure environment for staff to work and provide the best clinical care for service users. Employees failing to observe this policy and applicable health and safety regulations may be subject to action in accordance with the AWP Disciplinary Policy and procedures.

In order to minimise the risk of violence and aggression the Trust will work to implement its statutory duties highlighted by the Security Management Service (SMS). The Trust also recognises that it is important, so far as is reasonably practicable, to:

- Provide and maintain equipment and systems of work / procedures that are safe and without risks to health.
- Provide safe access and egress at places of work under the Trust's control that are safe and which minimise risks to health. Maintain places of work under the Trust's control in a condition that is safe and without risk to health.
- Co-operate with other agencies where Trust staff may be working within their premises.
- To enhance premises security, where fitted, door combination codes will be changed on a 6 monthly basis, or when security has been breached.

- Members of staff, when on Trust premises, will display their identification badges in a visible manner, for all to see. However, it is accepted that certain groups of staff do not wear their ID badges round the neck or pinned to the uniform as this could constitute a risk of injury to the individual or to the service user. Where appropriate, therefore, these members of staff may carry their identification badge, whilst on Trust business.

4. Scope

This policy shall apply to all security issues/procedures. It applies to all employees and non-executive directors of the Trust and to agency staff, service users, carers, contractors, volunteers, visitors and any other persons having lawful reason to be on Trust premises. The policy equally applies to staff and services of the Trust that are provided in community situations where staff are seconded to other healthcare organisations or people who are on work experience or training placement.

The policy will apply to all "workplaces" which will include: -

- All Trust premises
- All premises where staff are required to work, which are the management responsibility and/or are in the ownership of other organisations or individuals are expected to adopt Security arrangements.

5. Arrangements

5.1 Local Security Arrangements

The Trust has a variety of arrangements in place for security at its different sites, ranging from:

- dedicated contracted security staff
- security staff support through contractual arrangements
- no dedicated security arrangements in place
- Local procedures to ensure staff are aware of their duties, how to call for help and how to ensure security of the premises.
- Local procedures to ensure personal security, e.g. as described in Lone Working Policy and Recognition, Prevention and Management of Violence and Aggression Policy.

5.2 Security of Information

Please refer to the Information Governance Policies and protocols (see Associated and Related Procedural Documents).

5.3 Site Security

General site security is an issue for all staff and a general level of awareness is essential. Any untoward findings should be reported immediately to the manager responsible for the site and/or service.

All members of staff should ensure that their work areas are secured at the end of the working day (where applicable) and that departmental keys are held in a secure place at all times.

The Trust takes no responsibility for damage to or theft from vehicles parked on Trust property.

Each inpatient team/building must have an agreed procedure for the issue of keys, fobs and alarm units (as appropriate) which manages the issue of these items to staff, logs issue and return and ensures that all units are accounted for. An example procedure and template forms are shown in Appendix A – Lockdown Procedure, Appendix C – Procedure for the Allocation of

Keys, Alarms and Fobs (sets), Appendix D – Key Cupboard Handover Form, Appendix E – Set Control Form and Appendix F – Sets out of Circulation Form

On induction all members of staff will be provided with an identity badge that they will be expected to carry with them at all times.

Members of staff, who require access through any door, which is controlled via digital door locks or proximity access systems, will be issued with the appropriate code numbers or personal fobs/cards to ensure the security of the area is maintained at the highest level. Code numbers must not be issued to unauthorised personnel wishing to enter any premise who are not Trust employees, including Service User and Carer Representatives. Agency workers and volunteers acting in the capacity of employees will be issued with codes after appropriate security checks have been completed. Visiting staff to another AWP building will have to comply with the local arrangements regarding access, they will not be given codes to areas controlled by digital locks or proximity access systems. Any unauthorised individual attending any AWP sites will be escorted at all times by an authorised member of staff irrelevant of the reason for the visit, i.e. opening a unit, fund raising, auditing, this list is not exhaustive,

All code numbers must be kept secure and not issued to unauthorised persons requesting access to ensure security is maintained at the highest level.

All access codes will be changed:

- every 6 months, or
- whenever it is felt that the code may have become compromised, or
- on the termination of staff employment especially when security related.

The manager with designated responsibility for this area / building must ensure that this work is undertaken.

Lost ID Cards must be reported immediately; also if Personnel Access Control Cards or keys are lost this must be reported as soon as practicable in order that the card can be deactivated from the access system to ensure premises can be secured. An incident report form is to be completed.

Security Passes are personal to the user and should not be passed to unauthorised personnel or loaned to other members of staff. Security passes should not be issued to Service User Carers Representatives.

Members of staff should be aware of anyone trying to ‘tailgate’ – i.e. gain access to a controlled access area by closely following them as they enter. If the person is not recognised as a member of staff, or authorised visitor, he/she should be asked to:

- Wait at the door or in a designated waiting area
- Give details of the person, with whom they have an appointment.
- Await the arrival of an identified member of staff to escort them into the controlled access area.

At the end of the appointment / meeting, the visitor should be escorted out of the controlled access area.

5.4 Lockdown

In line with its responsibility to ensure a safe and secure environment, the NHS SMS has developed guidance to explain the planning and execution of a lockdown in NHS healthcare site. The term “lockdown” is used to refer to: “Controlling the movement and access – both entry and exit - of people including NHS staff, service users and visitors, around a Trust site or facility in response to an identified risk, threat or hazard that might impact upon the security of service users, staff, visitors and assets or the capacity of that facility to operate. A lockdown is achieved

through a combination of the physical security measures and in some areas, the deployment of security personnel.

A Lockdown should be used to ensure the safety and security of all Trust personnel, service users, visitors, property and assets in the event of a major incident and by doing so will protect the integrity of the Trust. (refer to Lockdown Procedure - Appendix A)

5.5 Office and Desk Security

The occupier of an office and desk is responsible for confidential information contained therein, especially when others may have access to the office after hours. Members of staff must, therefore, ensure that:

- A “clean desk” policy is implemented, to help prevent the theft of confidential information.
- Confidential information is not displayed on computer screens or left on the desk when the office is unoccupied, even for short breaks and that any computer screen is locked or a password-protected screensaver is activated.
- Any web deployed system, which contains confidential information, is shut down before leaving the computer.
- Doors and windows are locked, when leaving the office unoccupied, even for short breaks.
- All confidential material is kept securely.
- Confidential documents are always shredded, not discarded in the waste bin.
- The fax machine is installed in an area that service users/relatives/members of the public do not use (i.e. a safe haven).
- Fax cover sheets include a statement that notifies the receiver if confidential information is being transmitted. These can be found in the Data Protection Policy (including Subject Access Request and Safe Haven Procedures)
- Discussions of confidential information, in informal settings (e.g. the reception area) are limited.
- Ideally, the receptionist should have an area where telephone conversations cannot be overheard by service users / relatives / members of the public in the waiting area.
- When a request to access confidential information is made, it should never be disclosed unless the request meets the requirements of The Trust’s policy for disclosure of such information. Please refer to the Data Protection Policy (including Subject Access Request and Safe Haven Procedures)
- Only those authorised workers that need to access confidential information should be allowed to use Trust offices and desks where there is confidential information.
- When unoccupied curtains or blinds are drawn and windows and doors are secured.

5.6 Visitors

Where applicable:

- All visitors including visiting staff, Service User Carer Representatives and Volunteers must report to the reception area on arrival.
- Visitors must sign the visitor's book recording their name, business, the person they are visiting, time of arrival and departure.
- Visitor badges will be issued to all non AWP employees on official Trust business. Anyone suspected of not following the correct signing in procedures will be challenged and, if necessary, escorted to the reception, in order that the signing in process can be completed.
- Once the visitor has signed in, he/she must wait until the person, with whom they have an appointment, arrives to escort them to their destination. At the end of the meeting, the visitor will be escorted back to the reception area to sign out, prior to departure.
- Visitors must not be left unaccompanied with the exception of external organisations who may need to visit the building on official business taking account of prevailing health and safety risks. This will be at the agreement of a relevant Director or local Manager.

5.7 Service Users Property

The Trust will not accept responsibility or liability for Service Users property brought into in-patient units, unless it is handed in for safe custody and a copy of an official patient's property receipt is obtained. As per AWP Standing Orders and Standing Financial Instructions P113

5.8 Security of Drugs and Prescription Pads

All staff working within the Trust who are involved in some way with the use of medicines, must familiarise themselves with the correct procedures contained in the Trusts Medicines Policy P060 to ensure that medicines are handled in a safe and secure manner.

5.9 Criminal Offences and Police Involvement

When a criminal offence is committed or alleged to have been committed on Trust premises by any person the Police must be informed. The Senior Manager (on call manager for out of hours) must also be informed immediately.

The Trust will cultivate good relationships with the local Police and, in order to pursue the objectives of this policy, will actively seek to prosecute any individual who wilfully damages property or inflicts harm to any member of staff or service user.

If there is any suspicion of fraud, a report should also be made, in parallel, to the Director of Finance who will inform the NHS Protect Local Counter Fraud Officer.

All crimes must be reported via the incident reporting procedures without delay.

The manager will inform the appropriate Service manager / Director immediately with information in respect of the offence, and information in regard to the action taken. The Trust's LSMS should be informed as a matter of urgency with information in respect of the offence, details of police involvement and any action taken to date.

All reported incidents will be subject to the incident investigation procedures. Misconduct of employees whether admitted or denied, should be processed in accordance with the Trusts disciplinary policies.

Where theft or damage is related to property belonging to other persons i.e. patients, visitors or contractors, the Police will normally be advised.

5.10 Risk Assessment

The Management of Health and Safety Regulations 1999 places a specific duty on employers to carry out risk assessments on the hazards that employees may be exposed to and determine what control measures need implementing to avoid or minimise the risks in so far as is reasonably practicable.

In compliance with statutory requirements and the directions of the Secretary of State to NHS bodies, risk assessments should be undertaken to ensure the:

- Physical security of the ward/department.
- Physical security of the assets and property in the ward/department.
- A risk assessment of physical security of premises and assets will be undertaken on an annual basis and also on change of use.
- An assessment of personal alarm provision including the type, operation and number of handsets available and required.
- Personal safety of staff, service users, carers and visitors in the ward/department and grounds.
- Personal safety of staff based in the ward/department but working outside the premises.

Security risk assessments will be undertaken locally as indicated and required, e.g. following a change of use of the building, and as part of the regular risk assessment activity.

The Trust's approach to risk assessment is described in the Risk Assessment Policy and this includes a template for risk assessments. The checklist for security risk assessment and interview room assessment are described in Appendices A & B of the Violence Reduction and Management policy.

Additional guidance is given on the Trusts Violence and Aggression and Security Risk Assessment Pages (part of the monthly statutory risk assessment schedule) which describe the process for assessing security risks. Security risks can be identified by using the Check List for Physical Security Risk Assessments and where risks are highlighted these can be assessed using the Trusts Standard Risk Assessment forms.

Action plans will be developed as a result of security risk assessments to identify priority activity areas. The risk assessment template requires actions to be identified where risks have been found, risk rated and controls have been considered. Each item is assigned a target date to assist in reviewing actions taken and prioritising work.

Many risks will be able to be managed within the team and local resources, Items identified as requiring priority attention and not able to be resolved at a local level will be escalated to the service's management group supported by the service Health and Safety Group and or Hub Group as necessary. Ongoing risks may need to escalate through local, service and Trust risk registers as necessary. The process for escalating and reporting risk is shown in Appendices 2 & 3 of the Trusts Health and Safety Policy

Service and Trust risk registers are reviewed regularly by the Trustwide Management Group and the Health, Safety, Security and Fire Group as appropriate. Less significant risks managed within the team shall be monitored by the line manager as part of ongoing review of all safety actions. Additionally scrutiny of risk assessments and action plans form part of the overall security and health and safety audits programme

When carrying out a risk assessment practical advice and support may be obtained from the Trust LSMS, Head of Health and Safety and Health and Safety Advisers.

5.11 Estates and Facilities Management Works

In the planning of re-development or provision of new buildings/facilities for Trust premises, due regard will be given to ensure that security management is considered at the design stage.

Appropriate representation is sought for all project steering groups and this must include appropriate representation from the Health, Safety, Security & Fire Group. All works will meet NHS Estates Health Building Notes and Health Technical Memoranda.

All directorates will ensure that appropriate liaison takes place.

6. Definitions

The term “security” will apply to the elimination or reduction of the risk of crime in all its forms within the Employing Organisation. It will apply to:

- Crimes against individuals – violence and abuse. (See Recognition Prevention and Management of Violence and Aggression Policy).
- Damage to and theft from premises. (See Standing Financial Orders).
- Theft or misappropriation of drugs. See Medicines Policy).
- Security of information. (See Data Protection Policy).
- Security of computer held information (Acceptable Use Policy).

7. Roles and responsibilities

7.1 Executive Management

The Trust Board is ultimately responsible for fulfilling legal requirements relating to security and it vests in the Chief Executive responsibility for the fulfilment of the relevant statutes

7.2 Responsibilities of The Chief Executive

The Chief Executive takes specific responsibility for:

- Advising the Trust Board on the review of existing policy arrangements and allocation of resources to implement security related procedures.
- Referring matters of a critical nature to the Trust Board for resolution and ensuring that adequate security arrangements exist within the Trust.

7.3 Non Executive Director

The requirement for a Non Executive Director (NED) is set out in Secretary of State Directions to NHS Bodies on Security Management Measures 2004 (amended 2006). The role of the NED is to support, and where appropriate, challenge and support the Security Management Director on issues recommendations relating to security management at Executive Board level. This role is undertaken by the Chair of the Trust

7.4 Executive Directors

On behalf of the Chief Executive the Director of Nursing, Compliance, Assurance and Standards takes lead responsibility for the management of Security within the Trust.

The Director of Nursing, Compliance, Assurance and Standards is also the nominated Security Management Director (SMD) and is the lead for Security at Board level. This is to ensure the monitoring of and compliance with Secretary of State Directions and subsequent guidance; and the requirements of the NHS SMS in relation to measures taken to provide for effective Security Management.

The SMD will be responsible for ensuring:

- Promotion of safe working in all Trust operations.

- Overall responsibility for the accredited Local Security Management Specialist (LSMS) to ensure that security management work is undertaken to the highest standard.
- Overseeing the introduction, operation, monitoring and evaluation of this policy to ensure comprehensive, fair and consistent application throughout the Trust.
- In conjunction with the other Executive Directors, the provision of training, guidance and support to managers on the implementation of this policy.
- Arrangements exist for the circulation of Regulations and Approved Codes of Practice (ACoP) and to act on reports from Trust Specialist Advisors, Safety Management Group and the Health and Safety Executive (HSE).
- Systems exist to maintain records of accidents and dangerous occurrences and the reporting of incidents.
- Employees are allocated clear responsibilities and receive adequate training in accordance with this policy.
- Reports and audits on security related issues within the Trust are produced for consideration at the Health, Safety, Security & Fire Group and subsequent review at the Safety Management Group.

7.5 Responsibilities of the Director of Human Resources

The Director of Human Resources has the responsibility for directing how alerts received from NHS Protect relating to rogue staff are disseminated within the organisation and for ensuring that the appropriate steps are taken to address any HR issues highlighted by alerts.

The Director of Human Resources has overall responsibility for learning and development and will ensure that an appropriate programme of security training is made available to all staff commensurate to their role within the organisation. The training records of staff attending the Trust's violence and aggression training are held with the Learning and Development department.

7.6 Responsibilities of the Director of Nursing,

The Director of Nursing iIs responsible for the collation and reporting of all incidents and for working jointly with the Head of Patient Safety Systems, Nursing and Quality and the LSMS to ensure that appropriate investigations and actions are taken

7.7 Responsibilities of All Directors, Associate Directors and Operational Manager & Clinical Leads

All Directors, Associate Directors and Operational Manager & Clinical Leads are responsible for ensuring that for each service and department within their directorate/division:

- Compliance with this policy and associated policies throughout their areas of responsibility and local arrangements that implement this policy are devised and reviewed.
- Thorough risk assessments, specifically focusing on maintaining a secure environment and the physical security of premises and assets, are included within their directorates risk assessment processes
- Appropriate provision of resources and training is made available to address the outcomes of assessments or incident investigations. The Trust will attach a high priority to supporting investments put forward as a result of the risk assessment process whilst recognising the financial constraints of the organisation.
- Adequate security arrangements are in place for all sites where they provide services or accommodation for staff.

7.8 Responsibilities of Line/Ward Managers & Team Leaders

Each line manager has key responsibilities to ensure:

- Within their area of responsibility, that this policy is complied with and that employees are sufficiently aware of and conversant with this policy to perform their duties.
- Managing their wards, teams and departments to ensure that local security arrangements contribute to a secure environment.
- Provide appropriate alarm, communication equipment and procedures and ensure that they are properly used. Systems should provide for checks to identify faults and ensure that prompt remedial action and maintenance is carried out. Records of tests, checks and maintenance should be kept.
- All staff adhere to the Incident Management Policy.
- All relevant staff are conversant and comply with the Health & Safety for Lone Working Policy.
- Providing support and advice to staff following notification of an adverse event or security incident.
- Suitable and sufficient security risk assessments regarding the physical security of premises and assets are carried out within their ward/department and clearly documented and amended in an appropriate format where necessary. Additional guidance is given on the Trusts Violence and Aggression and Security Risk Assessment Pages (part of the monthly statutory risk assessment schedule) which describe the process for assessing security risks. Security risks can be identified by using the Check List for Physical Security Risk Assessments and where risks are highlighted these can be assessed using the Trusts standard Risk Assessment forms
- Seeking advice from the Trust LSMS to ensure incidents are investigated and appropriate action arising from the investigations is taken.
- Completing the Security section of the annual Health & Safety audit and co-operating with other audits as required.
- Undertaking periodically the security element of the risk assessment check list as part of overall health and safety duties.
- Ensure that the issue of keys, fobs and alarms are managed appropriately so that keys for all inpatient units these are accounted for and that the team has a local procedure in place to manage these appropriate to the risk (refer to Appendix C – Procedure for the Allocation of Keys, Alarms and Fobs (sets), Appendix D – Key Cupboard Handover Form, Appendix E – Set Control Form, Appendix F – Sets out of Circulation Form and Appendix G – Battery Changing Record Form) for an example procedure and management templates).
- Regularly check that the local key, alarm and fob procedure is being implemented and that all keys and fobs are secure and that there are sufficient alarm handsets for the environment.
- Ensure that a local Lockdown procedure is in place and communicated to staff (See Appendix A – Lockdown Procedure

7.9 Responsibilities of Individual Employees

The policy requires all employees to:

- Co-operate in measures and procedures to ensure the provision of a secure environment.
- Report all adverse events to their line manager and completing an incident report form as appropriate in accordance with The Policy for the Reporting, Management and Investigation of Adverse Incidents (including Serious Untoward Incidents) (Also known as The Incident Policy)
- Report suspicious packages or individuals to their line manager.

- Have due regard for their own security as well as that of other members of staff, service users, carers and visitors by the proper use of all security facilities such as locks and alarms.
- Follow local procedures on the issue of fobs, keys and alarms
- Trust employees have a responsibility to alert other organisations if they believe there is a risk that others will be exposed to violent or aggressive behaviour

7.10 Local Security Management Specialist (LSMS)

An accredited Local Security Management Specialist will, on behalf of the Trust, be responsible for taking all necessary action as described in the Secretary of State Directions (2003) amended directions (2006). This will include ensuring:

- Support, advice and guidance is provided to all staff in measures to deal with Security Management.
- The SMD is kept fully informed on issues relating to Security Management which may affect the Trust, its staff, service users or the levels of service which it offers.
- That the role acts as a central point of contact within the Trust for the Police in respect of security management, to ensure that relevant information is communicated and effective action is taken in the detection and prevention of crime and disorder.
- That incidents relating to security matters are reviewed and providing reports on trends and security management performance.
- Monitoring effectiveness of any local security arrangements is undertaken
- Security surveys and risk assessments as is necessary are commissioned to protect people and property.
- That collaborative working takes place with the Learning and Development Team to ensure that effective training in the management of violence and aggression and general security is available to all staff and non-executives who require it.
- That collaborative working takes place with the Trust Local Counter Fraud Specialist when necessary in accordance with standing financial instructions.
- Trust leads are informed of Security issues that impact upon their portfolios

7.11 Health, Safety, Security and Fire Group

The Health, Safety, Security & Fire Group reports to the Safety Management Group and is chaired by an Executive Director; In terms of security it is responsible for ensuring that:

- It meets regularly to assure that there are effective security management processes in place to comply with legislation and national guidance.
- The LSMS' work plan is approved.
- The Security Management annual assurance report for the board is developed and agreed
- Any other matters relevant to security management work are discussed in accordance with legislative requirements and ensuring appropriate bodies are informed of change.
- An organisation wide action plan based on security assets risk assessments and audits is developed and maintained and improvements monitored on a two monthly basis.
- The action plan will be forwarded to all Directorates and Support Service Business Managers for action. The organisational action plan will be updated on receipt of assurance reports and reviewed monthly as part of the Health, Safety, Security and Fire Groups work plan.
- The effectiveness of all security management arrangements in the Trust is monitored.
- There are effective security management processes in place within all directorates and services.

- Staff security, personal safety and specialist security training is monitored,
- Implementation of Security Management plans is monitored.

The implications of new legislation and initiatives in particular from NHS Security Management Service, Health and Safety Executive and National Institute for Clinical Excellence are acted upon.

7.12 Occupational Health

The Trusts Occupational Health Providers liaising with Employee Support Services shall offer a confidential, independent and free counselling service to which employees may seek access on a self referral basis

The Trusts Occupational Health Providers shall complete health assessments for employees returning to work where referred by their manager in order to establish fitness for work and in accordance with Disability Discrimination legislation and suggest reasonable adjustments to reduce the risk.

8. Training

The Trust's overarching policy for training is the Learning and Development Policy and this should be read in conjunction with this policy. Attached as appendices to that policy are the Trust's learning and development matrices. These matrices describe the minimum statutory, mandatory and required training for all staff groups in respect of manual handling training.

The Learning and Development Policy also describes the Trust's arrangements for training, in particular how there are processes in place to ensure staff receive the training they require and how non-attendance is followed up. These arrangements are further supported by management supervision and appraisal processes.

The Trust lead for security has agreed the training standard with the Learning and Development Team and training standards have been informed by statutory requirements, professional standards and national best practice.

The Trust lead for security participates in a programme of continuous professional development to ensure they remain up to date and keep abreast of developments in this field.

The Trust will have an accredited LSMS trained by the Security Management Service.

External providers of Security staff will be responsible for the training of its staff. This will be monitored on a regular basis through Security Contract Meetings.

Training related to violence and aggression are described in the P095 Violence reduction and management policy

9. Monitoring or audit

Implementation of this policy will be measured by a number of indicators including risk assessment activity via the Statutory Risk assessment schedule and team level returns from the annual health and safety assessment process. This enables the Trust to provide external bodies such as the NHS Litigation Authority, Health and Safety Executive and the Healthcare Commission with evidence and assurance of compliance with standards.

- The LSMS will monitor and review trends in security incidents across the Trust and prepare analytical reports for the Health, Safety, Security & Fire Group.
- The Health, Safety, Security & Fire Group will monitor the implementation of this policy in terms of effectiveness and performance by reviewing incidents and trends. It will monitor convictions, staff and patient injuries as a result of violence. These are also reported in the six monthly incident report received by the Quality and Healthcare Governance Committee.

- Participating in external audits annually, conducted by the SMS and benchmarking Trust performance against others. These are reported to and monitored by the Health, Safety, Security and Fire Group
- Monitoring staff views and trends via Staff survey and Stress assessments. These are undertaken every 2 years and reported via the Modernisation and Workforce Management Group, the Safety Management Group and the Quality and Healthcare Committee.
- Monitoring of team level returns from the Annual Health & Safety Self Assessment process. These monitor key aspects of the management of safety regarding management of violence and aggression, building security including Lockdown, environment and training. Data from these is monitored by the Health, Safety, Security and Fire Group annually which sets work plans based on key risks identified during the annual health and safety self assessment process and a combination of external and internal security audits. The results are reported to the Quality and Healthcare Governance Committee in the Annual Health, Safety and Security report.

10. References

Additional guidance is given on the Trusts Violence and Aggression and Security Risk Assessment Pages which describe the process for assessing security risks.

Security risks can be identified by using the Check List for Physical Security Risk Assessments and where risks are highlighted these can be assessed using the Trusts standard Risk Assessment forms.

This Policy should be read in conjunction with the following legislation, regulations and Trust policies:

- Health and Safety at Work Act (1974)
- Data Protection Act 1998
- Management of Health and Safety at Work Regulations 1999 ISBN0110856252
- Violence. The short term management of disturbed/violent behaviour in psychiatric in-patient settings and emergency departments (NICE, 2005)
- The Civil Contingencies Act 2004

11. Associated and Related Procedural Documents

Violence Reduction and Management Policy

Risk Assessment Policy

Health & Safety Policy for Lone Working

Learning and Development Policy

Disciplinary Policy

AWP Capability & Conduct Policy & Procedure for Medical Staff

Dignity at Work Policy

Medicines Policy

Incident Management Policy

AWP Standing Orders and Standing Financial Instructions

Acceptable use Policy

Major Incident Plan

Data Protection Policy

Health and Social Care Records Policy

Information Security Policy

Records Management Policy

Overarching Information Governance Policy

Freedom of Information Policy

Procedure - Handling Requests under the Freedom of Information Act

Hostage and Safety Guidelines for Hostage Situations

Counselling Advice available PAM

Check List for Physical Security Risk Assessments

12. Appendices

Appendix A – Lockdown Procedure
Appendix B – Not currently used
Appendix C – Procedure for the Allocation of Keys, Alarms and Fobs (sets)
Appendix D – Key Cupboard Handover Form
Appendix E – Set Control Form
Appendix F – Sets out of Circulation Form
Appendix G – Battery Changing Record Form

Version History

Version	Date	Revision description	Editor	Status
1.0	17/12/2008	Approved by Board	DB/PAD	Approved
2.0	05/01/2010	Ratified by Quality and Health Care Governance Committee	DB/PAD	Approved
3.0	06/07/2010	Ratified by Quality and Health Care Governance Committee	DB/PAD	Approved
4.0	04/12/2012	Approved by the Quality and Safety Committee	DB/PAD	Approved
4.1	16/07/2014	Amendments to Section 5.3 – Site Security	DB/PAD	Draft
5.0	17/02/2015	Approved by Quality and Standards	DB/PAD	Approved
5.01	26/01/2018	Draft for Health, Safety, Security and Fire Group	PAD	Draft
6.0	28/01/2018	Approved by the Health, Safety, Security and Fire Group	PAD	Approved