Cumbria Partnership NHS
NHS Foundation Trust

Security Policy

Document Summary

Cumbria Partnership NHS Trust will identify and address risks to staff, service users, and members of the public, and risks to property and assets, arising from acts of violence, aggression or any other form of security breach, in order to develop a secure work environment and a pro-security culture.

DOCUMENT NUMBER	POL/002/015
DATE RATIFIED	October 2015
DATE IMPLEMENTED	October 2015
NEXT REVIEW DATE	October 2018
ACCOUNTABLE DIRECTOR	Director of Strategy and Support Services, Executive Lead and Accountable Officer for Finance
POLICY AUTHOR	Safety and Security Officer

Important Note:

The Intranet version of this document is the only version that is maintained.

Any printed copies should therefore be viewed as “uncontrolled” and, as such, may not necessarily contain the latest updates and amendments.

Here for you

TABLE OF CONTENTS

1 SCOPE

This policy applies to all Trust-employed staff, all staff working in integrated teams, full-time and part-time clinical and non-clinical staff, staff directly employed and those who may be contracted-in. This policy covers all security incidents as per the definition given later in this policy, including violence & aggression towards staff, patients or others connected with Trust services.

This policy will be implemented throughout the Trust and will be supported by local arrangements to maintain safe and secure work environments.

DRAFT

2 INTRODUCTION

Health and Safety at Work Act 1974 (HASWA), Management of Health & Safety at Work Regulations 1999 (MHSW), Service Condition 24 of the NHS Standard Contract 2015/16 and Care Quality Commission performance standards all provide a framework and standards to be adhered to.

Cumbria Partnership NHS Trust recognises and accepts that the management of security is an integral part of its statutory duties under HASWA and its subordinate legislation, Service Condition 24 of the NHS Standard Contract 2015/16 and other requirements. Security risks will be risk assessed, and where appropriate, sensible and cost effective security management initiatives to reduce risks to all stakeholders will be introduced to establish a pro-security culture that aims to deter and prevent criminal activity.

3 STATEMENT OF INTENT

Cumbria Partnership NHS Trust will identify and address risks to the security of staff, service users, and members of the public, including risks to property and assets, to develop a safe and secure work environment and a pro-security culture, thus assisting in delivering high quality clinical services. In particular, it seeks to ensure, as far as reasonably practicable:-

- The personal safety and security of service users, members of the Public and staff whilst on Trust premises, or when working elsewhere on Trust business.

- The protection of Trust assets, property and equipment, and that of service users, staff and, members of the Public, against theft and damage, whilst on Trust premises.

- That criminal activity is deterred and that there is an effective response to all security incidents.

- When appropriate to do so, that security incidents are reported to the Police where members of staff are injured, assaulted or harrased, and for all other security incidents relating to theft or damage to property, equipment or assets or other criminal offences relating to behaviour.

- That wherever practicable, the delivery of healthcare is uninterrupted following a security incident, and provisions are made in respect of major incidents.

- That the awareness of staff will be raised towards implementing a pro-security culture and adopting proactive security arrangements.

- That staff are fully supported when reporting incidents of violence, theft or damage or other security related incidents.

- That foreseeable significant risks in relation to security of Trust assets, property, equipment, employees, or people effected with the Trust's activities are assessed, appropriate control measures identified and implemented, and that these control measures are kept under review

4 DEFINITIONS

Local Security Management Specialist (LSMS)

An employee of the Trust who has been accredited by NHS Protect to act in the position of Local Security Management Specialist, to coordinate security management arrangements within the Trust and to investigate any serious security incidents that may occur. This is a statutory post with mandatory responsibilities.

Local Counter Fraud Specialist (LCFS)

An employee of the Local Counter Fraud Service who has been accredited by NHS Protect to act in the position of CPFT's Local Counter Fraud Specialist, to coordinate counter fraud arrangements within the Trust and to investigate any serious fraud incidents that may occur. This is a statutory post with mandatory responsibilities.

Police Single Point of Contact

A police officer who has been nominated to act as a liaison/point of contact between the Trust and the police force on security issues, for example following incidents or to provide background information regarding previous criminal history of service users coming into the service.

PREVENT Lead

An employee of the Trust who has been accredited by NHS Protect to act in the position of PREVENT Lead, to coordinate counter terrorism arrangements within the Trust and to investigate any allegations that may occur. This is a statutory post with mandatory responsibilities. The Trust PREVENT Lead is part of the Safeguarding Team.

DRAFT

Counter Terrorism Officer / Counter Terrorism PREVENT Lead

A member of the police who liaises with the LSMS on the delivery of Project Argus and in respect of any behaviour from staff, public or patient that is suspected to relate to terrorist or radical activity.

NHS Legal Protection Unit

An NHS Agency that provides legal services to NHS Bodies. Services include taking cases to Court for the prosecution of persons who have committed offences against the NHS.

Controlled Drugs or Weapons

Any drugs or substances that are classified as controlled under current legislation, any weapons or articles classed as illegal or dangerous under current legislation, or any other item the nurse in charge feels would present a risk of harm to that patient, other patients or staff.

Security Incident

- An incident or occurrence that results in any person, property or asset suffering injury, harm, damage or loss as a result of an act of violence*, criminal act or other intentional act.

- An incident or occurrence that had the potential to result in an injury, harm, damage or loss to an individual, property or asset, as a result of an act of violence*, criminal act, or other intentional act, but for whatever reason, was prevented.

- Any incident or occurrence that led to, or had the potential to lead to, a breach of security of confidential records (or other information security breach – please refer to Trust policy on Information Security for further information)

- Any incident or occurrence that lead to, or had the potential to lead to, a breach of the physical security of Trust premises or part thereof.

* Trust policy on Prevention & Management of Violence & Aggression (PMVA) provides more detail and guidance in relation to incidents involving violence and aggression towards staff, however, for ease of reference, any incident falling within the following definitions qualifies as a 'security incident' and must be reported and followed up in accordance with this policy;

Physical Assault

"any incident where staff are abused, threatened or assaulted in circumstances related to their work, involving an explicit or implicit challenge to their safety, well-being or health" (HSE)

DRAFT

"The intentional application of force to the person of another without lawful justification resulting in physical injury or discomfort". (NHS Protect).

Please note - this applies to all incidents involving physical contact with staff by patients, including incidents deemed as being clinically-related.

Some examples are provided below:

- spitting on or at staff
- pushing or shoving
- poking or jabbing
- scratching or pinching
- biting or squeezing
- throwing objects, substances or liquids onto a person
- punching or kicking
- hitting or slapping
- sexual assault
- incident where reckless behaviour results in physical harm to others

Non-Physical Assault

"The use of inappropriate words or behaviour causing distress and/or constituting harassment" (NHS Protect).

Some examples are provided below:

- Offensive language, verbal abuse and swearing
- Racist comments
- Sexual advances or comments
- Loud and intrusive conversation
- Unwanted or abusive remarks
- Negative, malicious or stereotypical comments
- Invasion of personal space
- Brandishing of objects or weapons
- Near misses i.e. unsuccessful physical assaults
- Offensive gestures
- Threats or risk of serious injury to NHS staff

DRAFT

- Intimidation
- Failure to adequately control animals/pets.
- Stalking
- Preventing staff from leaving
- Alcohol or drug fuelled abuse
- Incitement of others and/or disruptive behaviour
- Unreasonable behaviour and non-cooperation such as repeated disregard of hospital visiting hours
- Any of the above linked to destruction of or damage to property.

Harassment

"A course of conduct which amounts to harassment of another which they know or ought to know amounts to harassment of another". harassment' includes actions that cause alarm or distress to an individual. (see section 15 of this policy for further information.

Theft, Criminal Damage and Inappropriate Behaviour

Examples of non-person assault security incidents are as follows (NB this list is not comprehensive):-

- Theft of a computer from Trust premises.
- Windows in trust premises being broken deliberately.
- Loss of keys to Trust premises (or part thereof).
- Theft of Trust property from a member of staff's car whilst working in the community.
- An unsuccessful break-in attempt to Trust-occupied premises.
- Any person behaving in an inappropriate manner on Trust premises or grounds, e.g. hunting rabbits with dogs, using car parks for 'joy-riding', using Trust grounds for any other apparent illicit/illegal activity.

DRAFT

5 DUTIES

Service Condition 24 of the Standard Contract 2015/16 place duties upon identified post-holders in relation to security management. These are listed below together with details of additional post-holders with security management responsibilities under this policy.

5.1 Trust Board

The Trust Board has a corporate responsibility for the provision of a safe environment.

5.2 Chief Executive

The Chief Executive has overall Statutory responsibility for Security management within the Trust.

5.3 Nominated Non-Executive Director

The Nominated Non-Executive Director will support, scrutinise and, where appropriate, challenge the Security Management Director and Board on issues relating to security management where it is appropriate to do so, and to also promote security management issues at Board level.

5.4 The Director of Strategy and Support Services

The Director of Strategy and Support Services acts as the Trust's Security Management Director (SMD) and is accountable to the Trust Board for the effective implementation of the Security Policy. Duties of the SMD are to ensure adequate security management provision is made within the Trust. The SMD must also have regular liaison with the LSMS to ensure security management work is being undertaken to the highest standard.

5.5 Local Security Management Specialist (LSMS)

The Trust has more than one accredited Local Security Management Specialist, one of whom is nominated to act as the Lead LSMS and who coordinates and oversees the activities of other accredited LSMSs within the Trust.

LSMSs are responsible for assisting the SMD in ensuring implementation of the Security Policy. LSMSs work to national standards in key generic and priority action areas on issues ranging from strategic governance to holding to account. Duties of the LSMS include:-

- Providing advice to the Trust Board, Departments, Managers and Individuals on security-related matters.

- Ensuring breaches of Security are investigated where appropriate to do so and progressing cases for consideration by NHS Protect Legal Protection Unit

DRAFT

and/or the Trust's appointed solicitors, with a view to seeking sanctions against offenders.

- Ensuring significant risks in relation to security management, together with risk treatment action planes/recommendations are notified to the SMD, for onward notification to the Trust Board where appropriate.

- Providing security/crime prevention advice within the limits of their knowledge, calling upon the Police Crime Prevention officer where appropriate, liaising with Police, the Security Management Service and other security disciplines as appropriate.

- Providing information and reports that may be required by the Board, its sub-committees, senior management groups or other appropriate bodies.

- Annual completion of the Organisation Crime Profile and Security Management Self Review Toolkit (inclusive of a workplan) which is prepared in liaison with, and is approved by, the SMD. The work plan and annual report are submitted to the Corporate Fire, Health, Safety and Security Committee for governance assurance purposes.

- Ensuring regular liaison with NHS Area Security Management Specialist and attendance at the quarterly regional LSMS meetings (arranged by the Area Security Management Specialist).

- Ensuring annual submission of Reporting of Physical Assaults.

- Annual submission of NHS Protect's self-assessment against Security Management Standards

- The LSMS and LCFS will liaise on a regular basis to ensure a coordinated approach towards the counter fraud and security management issues within the Trust.

- Monitoring security related incidents and reports.

5.6 Professional Head of Estates, & Estates Officers

The Professional Head of Estates is responsible for the physical security of Trust premises, including making arrangements for premises to be made secure as soon as practicable in the event of damage presenting a security risk. Estates Officers involved in planning or organising new building works or refurbishment schemes must ensure liaison with the LSMS to ensure security issues are considered in the schemes. Estates Officers should also seek advice and support from the local police crime prevention officers where it is considered necessary and appropriate to do so.

5.7 Heads of Department and all Managers

Managers are responsible for ensuring the implementation of this policy at local level. In particular they must:-

DRAFT

- Ensure that risks to the security of Trust property, premises and assets as well as the safety of service users, staff and members of the Public are reflected in all appropriate departmental procedures and risk assessments (which must be undertaken in accordance with the Policy for Service Delivery Health and Safety Risk Assessment).

- Inform the Head of Estates (or other appropriate officer if premises are not maintained directly by Estates) of any changes within their Department that affects the security of the premises, e.g. reporting of defects, faults with alarm systems and seek / implement immediate remedial actions .

- Ensure that Staff within their Department are instructed in security procedures for the ward/unit/department, including access control arrangements to restricted areas.

- Keep a record of all keys issued to (and returned from) staff in their Department.

- Ensure all security incidents (as defined within this policy), including loss of keys or other security breaches, are reported in accordance with this policy and also Trust's Policy for Incident and Serious Untoward Incident and Near Miss Reporting.

- Ensure that staff within their department are instructed to wear Trust ID badges at all times.

- Maintain a register of all valuable equipment used within their department, including that which belongs to the department but is used elsewhere by their staff, recording details such as make, model, serial number etc. Managers must also ensure that these items are appropriately stored to protect against theft or malicious damage when not in use.

- Ensure that any security alarm or device to protect property or staff is utilised and that any faults are reported to Estates for repair.

- Ensure that staff attend appropriate levels of training including relating to all aspects of security.

5.8 All Staff

All staff have the legal duty to comply with policies and procedures implemented by the Trust in the interest of safety and security. In particular, all staff must:-

- Be responsible for maintaining security in the area in which they work at all times, and highlight to their manager and/or the LSMS any security risks they become aware of.

- Fully co-operate with policies and procedures implemented to manage or affect safety and security.

DRAFT

- Report all security incidents including assaults, theft, criminal damage and other incidents of a suspicious nature to their Manager (and to the Police where appropriate) without delay. These must also be reported in accordance with the Policy for Incident and Serious Incidents which Require Investigation (SIRI) Policy.

- Wear a Trust ID Badge at all times and report the loss of such to their Manager immediately, in accordance with this policy and also the Trust's dress code policy.

- Report the loss of Trust keys to their Manager immediately.

- Take all reasonable steps to safeguard Trust property whilst in their care.

- Attend all necessary training relating to security.

5.9 Network / Care Group Governance Groups

Information on reported security incidents is available to Care Groups / Services on an ongoing basis through quality & safety dashboards. The Incident and Serious Incidents which Require Investigation (SIRI) Policy has for further information on governance of the incident reporting process.

5.10 Corporate Fire Health Safety & Security Committee

The Corporate Committee is the forum for formal consultation with staff and representatives on the Trust's Security management arrangements including the review and agreement of this Security policy. The Committee receives feedback on reported Security incidents, internal inspections, and also inspections undertaken by external enforcing/regulatory agencies which impact on security. It is responsible for monitoring and acknowledging performance on action plans developed following those inspections. The Committee is responsible for escalating any significant issues of concern to the Finance, Investment and Performance Committee or Quality and Safety Committee (depending on the nature of the concern). Issues of concern relating to training in personal safety are also referred to the PMVA Group for further attention.

5.11 Crown Prosecution Service (CPS)

The CPS decides whether cases go to court for offenders to be prosecuted based upon evidence provided to them by the police, or in some instances, by the LSMS, NHS Legal Protection unit or Solicitors acting on behalf of the Trust.

6 ARRANGEMENTS FOR SECURITY MANAGEMENT

6.1 Identifying and Recording of Security Risks

Security risks may become apparent in a variety of ways, including hazard identification exercises, following security incidents that occur, following inspections

DRAFT

that are undertaken of the workplace, or directly by staff who become aware of a security concern.

Where security risks are identified, these must be notified to the manager of that service area as soon as practicable, who must ensure a risk assessment is undertaken in accordance with the procedures described within the Trust Policy for Service Delivery Health and Safety Risk Assessment and actions are taken to control the risk as far as reasonably practicable.

Any significant security risk issues should also be notified to the LSMS, who will follow-up on the issue where appropriate to do so, which may include adding an entry onto the risk register where required.

Examples of security risks for which risk assessments must be undertaken include (NB this list is not comprehensive):-

- Ineffective or insufficient controls to restrict access into, or exit out of, a designated work area/ward.

- Situations or circumstances resulting in significant potential for theft or damage to trust property/premises/assets.

- Situations resulting in significant potential for harm to staff or others from violence / assault / harassment.

- Situations resulting in significant potential for breach of security of confidential information.

- Situations or circumstances involving the potential for radical behaviour.

DRAFT

6.2 Management of Identified Security Risks

The management of identified security risks will be detailed within the risk assessments and sometimes documented within local procedures. Risk assessments with ‘security’ as a risk type are summarised and presented in a report to the Corporate Fire Health Safety & Security Committee on at least an annual basis. That report shows actions taken and also those that are outstanding. All necessary further actions identified within risk assessments form part of an organisation wide action plan to reduce and manage risks. Progress with further / outstanding actions will be monitored and updated on an ongoing basis.

Risk assessments must be kept updated to reflect where actions have been undertaken or completed, and must be reviewed no less than annually. Please refer to the Policy for Service Delivery Health and Safety Risk Assessment for details as to the arrangements for an organisational overview of all risks, including risks to the security of premises and assets.

6.3 Reporting and Investigation of Security Incidents

All incidents falling within the definitions above must be reported to the relevant Manager (or their delegated deputy), as soon as practicable after the event, who must ensure appropriate immediate remedial / response action is taken. All security incidents must be reported in accordance with the Trust’s established incident reporting procedures, please refer to Trust Policy for Incident and Serious Incidents which Require Investigation (SIRI) Policy.

All security incidents resulting in serious injury or distress to staff members must also be notified to the Locality LSMS immediately following the incident. The LSMS will then follow up the incident with a further investigation as appropriate in liaison with the manager. Please see Appendix 1 for a flowchart as to how security incidents will be followed up by the LSMS.

6.4 Lone Working

Please refer to the Trust’s Policy for Lone Working for details of arrangements for lone working and supporting guidance.

6.5 Cash Handling

Where cash is handled on behalf of the Trust and/or patients, managers must ensure that any risks associated with this activity are assessed and appropriate control measures implemented accordingly. Procedures for handling of cash must be in line with Trust’s Standing Financial Instructions. Any discrepancies in cash should be reported to the Assistant Director of Finance immediately.

Minimum control measures are as follows:

- Two people must be present when cashing up and preparing cash for banking.

DRAFT

- Cashing up and preparing money for banking should not take place in view of the public.
- Cash must be stored in a locked safe that is secured to the floor/walls until banking takes place.
- At least two people must escort the money to the bank.
- Banking should be carried out regularly (daily for Community Hospitals with canteens).
- Times (and days if banking does not take place daily) and routes should be varied. Wherever possible the route to the bank should be taken by car.

6.6 Prevention & Management of Violence & Aggression (PMVA)

Please refer to the Policy for Prevention and Management of Violence & Aggression for further information on personal safety, and techniques to be used including breakaway and control and restraint. The monitoring of issues relating to the prevention and management of violence and aggression toward staff and patients, including the provision of PMVA training and incidents of violent assaults against staff will be via the Trust's Clinical Governance structures.

DRAFT

6.7 PREVENT

As part of the Governments revised counter terrorism strategy of June 2011 (CONTEST), the NHS has committed to support initiates to reduce the genuine risk we face from terrorism so that people can go about their lives freely and with confidence. It is made up of four work streams, or four Ps:

Protect - strengthening our borders, infrastructure, buildings and public spaces
Prepare - where an attack cannot be stopped, to reduce its impact
Pursue - to disrupt or stop terrorist attacks

The fourth P is ***Prevent*** which aims to stop people becoming terrorists or supporting terrorism. It has been described as "the only long term solution" to the threat we currently face from terrorism. The *Prevent* strategy will specifically focus on three broad objectives, known as the three I's:

- Respond to the **ideological** challenge of terrorism and the threat from those who promote it;
- Prevent **individuals** from being drawn into terrorism and ensure that they are given appropriate advice and support;
- Work with **institutions** where there are risks of radicalisation that we need to address.

Please refer to the Safeguarding Policy for further information on the PREVENT strategy.

6.8 Searching for Prohibited Items or Substances (Patients and Visitors)

The Trust operates a policy on the searching of patients and visitors for prohibited items or substances, such as controlled drugs or weapons. For further information please refer to the Policy on Management of Harmful Drugs.

6.9 Searching of Staff Suspected of Committing a Breach of Security

It is an offence for members of staff to permanently remove property belonging to the Trust without written authority. Failure to seek authority from line management could result in disciplinary action or criminal proceedings being taken.

If any member of staff is suspected of committing a breach of security through the possession of prohibited, controlled, or stolen items, they will be asked by their manager to consent to a search of their personal belongings, including lockers. Two members of staff as well as the individual concerned must be present at the time of the search. If the individual refuses to a search being undertaken, the manager will consult with HR Department regarding the possibility of instigating disciplinary proceedings.

6.10 Stalking and/or Harassment of Staff

In accordance with the Protection from Harassment Act 1977 “a person must not pursue a course of conduct which amounts to harassment of another which they know or ought to know amounts to harassment of another”. A ‘course of conduct’ means on at least two occasions, ‘harassment’ includes actions that cause alarm or distress to an individual. The ‘know or ought to know’ element of the definition is classed as what a ‘reasonable person’ would think. It is a criminal offence to breach this statutory requirement, with custodial sentences and/or fines being available to the Courts as a sanction against offenders.

Compared with the general population, clinical staff are at increased risk of being stalked or harassed, with doctors and mental healthcare professionals at greater risk of being stalked, particularly by their patients. Any member of staff who thinks they may be being stalked or harassed should report the matter immediately to their line manager and also to the LSMS for further advice.

6.11 Surveillance / CCTV

CCTV is installed in a number of Trust premises for the purposes of general security, for example monitoring entrances to the premises. The use of surveillance techniques, including the use of CCTV to specifically monitor any person, including staff who may be suspected of committing security-related offences, is not permitted without appropriate authorisation. Approval for directed or intrusive surveillance must be sought from NHS Protect via the LSMS, in accordance with Trust policy on Directed Surveillance. Please refer to the Trust’s separate more detailed CCTV Policy for further information.

6.12 Criminal Records Bureau (CRB) Checks

In order to minimise security risks to service users, staff and the Trust generally, the Trust applies a policy for undertaking Criminal Records Bureau (CRB) checks on people seeking paid or unpaid work with the Trust. The level of CRB check carried out on an individual will be dependent upon the nature of work they undertake. . Please refer to Criminal Records Policy for further information.

DRAFT

6.13 Security Licensing

Contracts for the provision of security services are organised through the Estates Department. The Head of Estates coordinates and monitors the use of appropriately Security Industry Authority (SIA) licensed security contractors.

6.14 Security Strategy – Priority & Generic Action Areas

NHS Protect have dictated priority and generic action areas where NHS Trusts must focus attention on security management issues. Current priority action areas are; Patients & staff, NHS property & assets, Maternity & paediatric units, and Drugs, prescription forms and hazardous materials. Generic action areas are; Strategic Governance; Inform and Involve; Prevent and Deter; Hold to Account.

The LSMS will submit an Organisation Crime Profile and a Self Assessment Review Toolkit to NHS Protect that states the Trust's actions to address these action areas. An annual work plan will be produced and signed off by the Security Management Director.

6.15 Security Alerts

NHS Protect occasionally issue security alerts to SMD's and LSMS's regarding people who they believe present a security threat to healthcare staff, patients using healthcare facilities, or premises or assets of the NHS. Upon receipt of these Alerts, the LSMS will notify appropriate designated managers throughout the Trust in order that they can cascade the information appropriately to areas that may potentially be affected.

6.16 Private Property & Vehicles on Trust Premises

Where a locker has been provided for personal use, the individual to whom it is allocated will be responsible for providing a suitable locking device.

Each Ward/Department/Unit must follow the Trust's procedure regarding the security of Service User's personal property/monies during their stay in hospital.

If private property has been lost or suspected stolen it is the owner's responsibility to report the matter to the relevant manager and also, if appropriate, to the police. The manager must then report the security incident using the Trust's incident reporting procedure, and must also notify Safety and Security, in order that the LSMS can be informed.

The Trust will take all reasonable steps to safeguard vehicles on its premises, however the Trust does not accept liability for the loss of, or damage to private property including motor vehicles or other modes of transport. Motor vehicles and other modes of transport are brought on to Trust premises entirely at the owners risk.

6.17 Key Security

All keys, including duplicates and spares must be accounted for in an auditable system, which should include obtaining signatures upon issuing keys, and recording their receipt/return. No additional keys should be cut without the approval of the Head of Estates or Departmental manager. Special arrangements should be made to protect keys that access specific stores, containers, or other secured area where it is considered inadvisable to place such keys in a central depositary or Departmental key cabinet respectively.

6.18 Purchase of Security Systems

Security systems e.g. automated access control systems (including video/intercom systems, swipe/proximity readers), CCTV, lighting and intruder alarms must be purchased with prior approval of the Head of Estates and liaison with the LSMS where considered appropriate. This will ensure compatibility of the system with existing systems and that other statutory regulations and guidance are complied with.

6.19 Major Incidents and Contingency Planning

The Trust has a major incident plan and each local area will have in place a localised business continuity plan. Further details and information relating to arrangements for Major Incidents and Business Continuity Planning are available from the Trust's Resilience Manager.

6.20 Lockdown

NHS Protect have issued guidance on 'Lockdown', which places duties on NHS Trusts to assess their security vulnerabilities in relation to locking-down a premises (or part thereof) in the event of a major security alert, or other event necessitating the restriction of movement into, out of, or within a premises. Please refer to Trust Preparing for Serious Security Occurrence (Lockdown) Policy for details of the Trust's arrangements in this regard.

6.21 Relationship with the Police and Other Agencies

If theft or malicious damage to NHS property is suspected to have been committed the Police will be informed either by LSMS or directly by staff in affected service area. When the personal property or interests of a Service User, member of Staff or visitor is affected because of crime, for example theft, damage or violent/ aggressive/ abusive behaviour whilst on Trust property or working on behalf of the Trust, both the individual and management have the right to call for Police assistance. Police will be given adequate facilities and full cooperation during the conduct of any investigation.

The LSMS will establish regular liaison with the following post-holders and agencies in the interests of promoting security management relationships and practices; SMD, Police Single Point of Contact for security matters; PREVENT lead, Counter Terrorism Officer, LSMS's in other NHS Trusts.

6.22 Inventories and Security Marking of Valuable Trust Equipment

Each ward/department/unit should create and maintain an inventory of all equipment considered to be of sufficient value or operational necessity to be marked. The value of the equipment to be included in the inventory should be determined by the Finance Department.

Valuable and/or attractive items of equipment, for example, IT equipment, televisions, videos etc. shall be marked to deter theft and assist in identification in the event if loss or theft. It items shall be marked by the IM&T Department; all other property shall be marked by the Department purchasing the equipment.

7 TRAINING

Mandatory training associated with security and prevention and management of violence and aggression is outlined in the Trust's Training Needs Analysis. Attendance at training is managed in accordance with the Learning and Development Policy.

The LSMS will also periodically deliver additional ad hoc instruction and/or information to staff on security management practices and security incident reporting arrangements.

8 MONITORING COMPLIANCE WITH THIS POLICY

The table below outlines the Trusts' monitoring arrangements for this policy/ document. The Trust reserves the right to commission additional work or change the monitoring arrangements to meet organisational needs.

Aspect of compliance or effectiveness being monitored	**Monitoring method**	**Individual responsible for the monitoring**	**Frequency of the monitoring activity**	**Group / committee which will receive the findings / monitoring report**	**Group / committee / individual responsible for ensuring that the actions are completed**
duties	Post holders are in place for Statutory posts defined by NHS Security Management Service	Head of Corporate Governance	Annual	Corporate Fire, Health, Safety and Security Committee	Associate Director for Corporate Governance/ Company Secretary

Aspect of compliance or effectiveness being monitored	Monitoring method	Individual responsible for the monitoring	Frequency of the monitoring activity	Group / committee which will receive the findings / monitoring report	Group / committee / individual responsible for ensuring that the actions are completed
arrangements for the organisational overview of the risk assessments regarding the physical security of premises and assets	Audit of risk assessment, incident & other data (e.g. assurance reports), •	Safety and Security Officer	Annual	Corporate Fire Health Safety & Security Committee	Head of Corporate Governance

9 REFERENCES/ BIBLIOGRAPHY

•

HSE 2007, *Management of Health and Safety at Work Regulations, L21*, HSE, London

NHS Security Management Service 2003, *A Professional Approach to Managing Security in the NHS*, Counter Fraud & Security Management Service, www.NHS Protect.nhs.uk

NHS Security Management Service, 2005, *'Not Alone – A guide for the Better Protection of Lone Workers'*, www.NHS Protect.nhs.uk

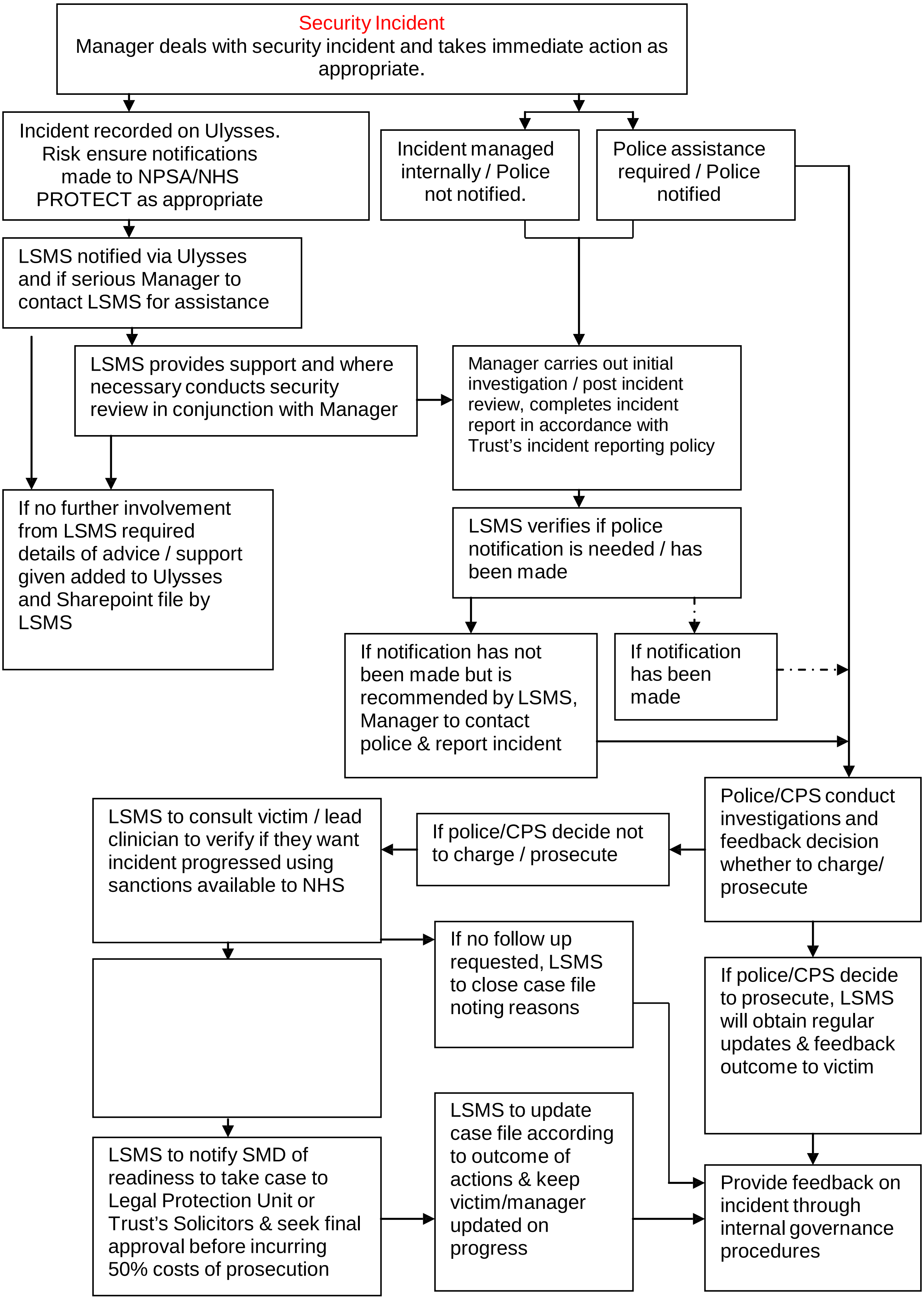
NHS Security Management Service, 2007, *'Tackling Violence Against NHS Staff'*, www.NHS Protect.nhs.uk

Standards for Providers 2013/4 Security Management www.nhsbsa.nhs.uk

10 RELATED TRUST POLICY/PROCEDURES

POL/002//019	Health and Safety Policy
POL/002/006I	Incident and Serious Incidents which Require Investigation (SIRI)
POL/002/010	Counter Fraud, Bribery and Corruption Policy
POL/002/023	Service Delivery Health & Safety Risk Assessment
POL/002/057	Lone Working
POL/001/008	Prevention & Management of Violence Aggression
POL/001/003	Searching of Service Users Person, Room or Personal Belongings
POL/004/027	Criminal Records Bureau
POL/002/070	Preparing for a Serious Security Occurrence (Lockdown)
POL/001/006	Safeguarding Policy
POL/002/077	Information Security Policy

APPENDIX 1 - SECURITY INCIDENT REPORTING & INVESTIGATION FLOWCHART



Security Incident
Manager deals with security incident and takes immediate action as appropriate.

Incident recorded on Ulysses. Risk ensure notifications made to NPSA/NHS PROTECT as appropriate

Incident managed internally / Police not notified.

Police assistance required / Police notified

LSMS notified via Ulysses and if serious Manager to contact LSMS for assistance

LSMS provides support and where necessary conducts security review in conjunction with Manager

Manager carries out initial investigation / post incident review, completes incident report in accordance with Trust's incident reporting policy

If no further involvement from LSMS required details of advice / support given added to Ulysses and Sharepoint file by LSMS

LSMS verifies if police notification is needed / has been made

If notification has not been made but is recommended by LSMS, Manager to contact police & report incident

If notification has been made

Police/CPS conduct investigations and feedback decision whether to charge/ prosecute

If police/CPS decide not to charge / prosecute

LSMS to consult victim / lead clinician to verify if they want incident progressed using sanctions available to NHS

If no follow up requested, LSMS to close case file noting reasons

If police/CPS decide to prosecute, LSMS will obtain regular updates & feedback outcome to victim

LSMS to notify SMD of readiness to take case to Legal Protection Unit or Trust's Solicitors & seek final approval before incurring 50% costs of prosecution

LSMS to update case file according to outcome of actions & keep victim/manager updated on progress

Provide feedback on incident through internal governance procedures