South Central Ambulance Service
NHS Foundation Trust

SECURITY POLICY

South Central Ambulance Service NHS Foundation Trust
Unit 7 & 8, Talisman Business Centre, Talisman Road, Bicester, Oxfordshire, OX26 6HR

DOCUMENT INFORMATION

Author:	John Dunn, Head of Risk and Security
Ratifying committee/group:	Health, Safety and Risk Group
Date of ratification:	January 2019
Date of Issue:	January 2019
Review due by:	January 2022
Version:	Health and Safety Policy (Appendix C) V6

Security Policy V6

Contents

1. Introduction

1.1 The South Central Ambulance Service NHS Foundation Trust recognises its duty to comply with the Health and Safety at Work Act (HSWA) 1974 and all subordinate regulations; and in particular the duty to provide a safe workplace that is secure for staff to provide healthcare. Therefore, the Trust is committed to ensuring, so far as is reasonably practicable, the health, safety and welfare of all of its employees and will do all that is reasonably practicable to protect staff and patients within its care from any security hazards.

1.2 The Trust is also committed to avoiding, so far as reasonably practicable, all security breaches/hazards and where it is not possible to do this carrying out suitable and sufficient risk assessments and crime reduction surveys to reduce the risk of a security breach so far as is reasonably practicable.

2. Scope

2.1 This policy applies to all who work for or carry out work on behalf of the Trust, including volunteers and work experience students. It also applies to all patients within the care and control of the Trust and any contractors and visitors whilst they are on Trust premises.

3. Equality statement

3.1 The Trust is committed to promoting positive measures that eliminate all forms of unlawful or unfair discrimination on the grounds of age, marriage and civil partnership, disability, race, gender, religion/belief, sexual orientation, gender reassignment and pregnancy/maternity or any other basis not justified by law or relevant to the requirements of the post. The Trust will therefore take every possible step to ensure that this procedure is applied fairly to all employees regardless of the afore mentioned protected characteristics, whether full or part time or employed under a permanent or a fixed term contract or any other irrelevant factor.

3.2 By committing to a policy encouraging equality of opportunity and diversity, the Trust values differences between members of the community and within its existing workforce, and actively seeks to benefit from their differing skills, knowledge, and experiences in order to provide an exemplary healthcare service. The Trust is committed to promoting equality and diversity best practice both within the workforce and in any other area where it has influence.

3.3 Where there are barriers to understanding; for example, an employee has difficulty in reading or writing, or where English is not their first language, additional support will be put in place wherever necessary to ensure that the process to be followed is understood and that the employee is not disadvantaged at any stage in the procedure. Further information on the support available can be sought from the HR Department.

4. Aim

4.1 The aims of the policy are to set out the arrangements for the identification, assessment and management of security hazards and risks to staff and patients (within its care and control); and contractors and visitors (whilst on Trust premises) and to provide and maintain a safe and secure working environment. It is also to protect the property (including medication and information property) and physical assets of the Trust

and its patients, staff and contractors and visitors whilst they are on Trust premises (including Trust vehicles).

4.2 The objectives are to ensure that the Trust has clear and defined arrangements for:

- the identification of security hazards and the protection of staff and patients and contractors and visitors on Trust premises
- the carrying out of suitable and sufficient risk assessments on security issues (including the threat of potential terrorist activity)
- the carrying out of crime reduction surveys to identify the treat to Trust property and patient's property from fraud, theft and wilful damage; and to identify the threat of potential terrorist activity
- the introduction and maintenance of controls to reduce the potential for theft, fraud and damage of Trust and patient's property and potential terrorist activity
- the management and control of risks from security hazards
- the regular review of these risk assessments and crime reduction surveys
- partnership working with agencies such as the Police, Local Authorities, the Crown Prosecution Service and NHS England.

5. Roles and Responsibilities

5.1 Trust Board

5.1.1 The Trust Board will ensure that there suitable and sufficient arrangements and adequate resources for the identification, assessment and management and control of the risks to staff and patients (within its care), volunteers, work experience students, contractors and visitors (affected by the activities of the Trust) from security breaches/hazards.

5.2 Chief Executive

5.2.1 The Chief Executive has overall responsibility for:

- the effective implementation of this policy within the Trust and for ensuring that there are suitable and sufficient arrangements for identification, assessment and management and control of the risks to staff and patients (within its care), volunteers, work experience students, contractors and visitors to the Trust from security breaches/hazards.
- ensuring the allocation of sufficient resources to maintain efficient and effective health and safety arrangements to provide and maintain a safe and secure working environment and prevent security breaches/hazards and incidents
- ensuring that policies are reviewed to secure compliance with existing legislation and any changes to this legislation.

5.3 Executive Director

5.3.1 Executive Directors are responsible for the effective implementation of this policy within their directorates and for ensuring that there are adequate resources available to fulfil the requirements of this policy.

5.4 Director of Patient Care and Service Transformation

5.4.1 The Director of Patient Care and Service Transformation is directly accountable to the Chief Executive and will advise and assist the Trust Board in fulfilling its duties under the relevant statutory legislation. The Director of Patient Care and Service Transformation is also the nominated executive Director with statutory responsible for overseeing security management work and ensuring compliance with the Secretary of States' Directions for security in the National Health Service (NHS). In particular they are responsible for:

- ensuring that workplace health, safety and welfare procedures are constantly reviewed
- ensuring that there are arrangements for liaising with the Health and Safety Executive (HSE) and NHS England
- ensuring that the Trust Board are kept abreast of relevant new legislation and guidance in order to ensure on-going compliance with the law
- the use of close circuit television (CCTV) within the Trust and for the registration of the Trust's CCTV system with the Data Protection Office.

5.5 Managers and Supervisors

5.5.1 Managers and supervisors' responsibilities include:

- attending any training to enable them to fulfil their responsibilities outlined in this policy
- bringing this policy to the attention of staff within their area of responsibility
- ensuring that all staff within their area or responsibility comply with this Security policy and any security protocols and procedures
- ensuring staff are issued with and wear identity badges/cards in such a way that they are visible
- ensuring that staff leaving the Trust return their identity badges, keys to Trust premises and their uniforms beforehand
- ensuring that they have effective arrangements in place for the security of keys with their respective areas of responsibility
- seeking advice on security matters, where necessary from the Trust's Local Security Management Specialists (Head of Risk and Security and the NonClinical Risk Manager)
- ensuring that all relevant staff within their area of responsibility attend initial conflict resolution training and refresher conflict resolution training
- encouraging staff within their area of responsibility to report all security issues and incidents, including any near misses, using the Trust's Incident reporting system, Datix
- ensuring that local procedures and protocols are developed as required to maintain the security and safety of all persons, property and information within their areas of responsibility
- communicating these local procedures and protocols to all staff within their areas of responsibility
- ensuring that staff have access to appropriate information and instructions regarding the security of personal property and Trust property and premises
- ensuring that members of staff are given all necessary support and advice in the event of them being assaulted

- co-operating with the carrying out of any risk assessments on security matters and any crime reduction surveys
- communicating the significant findings of these assessments and the crime reduction surveys to the staff within their areas of responsibility
- making arrangements to ensure, so far as is reasonably practicable, that all identified controls and further controls identified by the assessment and/or crime reduction survey any subsequent reviews are put into place
- making arrangements to ensure that all of the staff within their area of responsibility receive appropriate information about the significant security hazards and risks associated with the work they carry out for the Trust; and how to avoid such problems and what to do if problems occur
- arranging for the investigation of any security matters or incidents raised by the staff within their area of responsibility
- notifying the Risk Department immediately of any serious security issue within their area of responsibility
- where necessary, referring any staff who have being the victim of an assault whilst at work to Occupational Health for assessment.

5.6 All staff

5.6.1 Staff have the following responsibilities:

- to make themselves fully aware of the policy and to abide by it
- to ensure that whilst they are on Trust business or a Trust property they wear their identity badge so that it is highly visible
- to follow the Trust's and their site's specific procedures and protocols regarding the security of people, property, information and premises
- to challenge (politely) any unauthorised visitors found on Trust property and to report the matter immediately to their manager if they have any concerns about the visitors. When challenging such individuals, staff should do it at a safe distance so that they do not become a possible victim of violence
- to comply with any information, instruction and training provided for them to enable them to carry out their work safely and avoid any security breaches/hazards and incidents
- to take reasonable care for their own health, safety and security and that of others who may be affected by their acts or omissions
- to take reasonable care for the security of Trust property
- to co-operate with the Trust in relation to the completion of any risk assessment on security matters and/or any crime reduction survey
- to utilise any equipment provided to ensure their safety and security; and report any defects to this equipment using the Trust's Incident reporting system, Datix
- to adhere to any safety and security measures put in place to ensure their safety and security, including any safe systems of work or safe operating procedures
- to report any criminal activity, intentional criminal damage, security issue or security incident (including breaches and near misses) arising from the carrying out of their work using the Trust's incident reporting system, Datix. This includes reporting any incidents involving patients, contractors or visitors who have been affected by their work and which has resulted in a security issue/incident/breach/near miss

- to attend the Occupational Health department, if referred by their manager because of a physical assault.
- to ensure that before leaving their employment with the Trust they return their identity badge, any access keys and their uniform to their line manager.

5.7 Head of Risk and Security

5.7.1 The Head of Risk and Security is a trained and accredited Local Security Management Specialist (LSMS) and will be responsible to the Director of Patient Care and Service Transformation for the development of effective policies and procedures to assist the Trust in providing a safe and secure environment for staff and patients and thereby help to prevent security related issues or incidents. This should also help to reduce the number of potential claims for security matters.

5.7.2 The Head of Risk and Security will:

- devise an annual security management work plan and agree this with the Director of Patient Care and Service Transformation. This work plan will be shared with NHS England
- provide an annual written report on the activities of the Trust's Local Security Management Specialists based on the said work plan to the Director of Patient Care and Service Transformation, the Health, Safety and Risk Group.

5.7.3 As one of the Trust's two Local Security Management Specialists, the Head of Risk and Security has a number of other duties which are listed in the Local Security Management Specialist's responsibilities in section 5.9 below.

5.8 Non-Clinical Risk Manager

5.8.1 The Non-Clinical Risk Manager is a trained and accredited Local Security Management Specialist and will assist and support the Head of Risk and Security and the Trust in carrying out security work in accordance with the training and requirements of the Secretary of State's Directions and NHS England.

5.8.2 The Non-Clinical Risk Manager will provide a report on reported security incidents to every Health, Safety and Risk Group meeting.

5.8.4 As one of the Trust's two Local Security Management Specialists, the Non-Clinical Risk Manager has a number of other duties which are listed in the Local Security Management Specialist's responsibilities in section 5.9 below.

5.9 Local Security Management Specialist's responsibilities

5.9.1 The Trust has two trained and accredited Local Security Management Specialists (LSMS) and these are the Head of Risk and Security and the Non-Clinical Risk Manager. Both of whom will work in accordance with the relevant Secretary of State Directions and the training, guidance and advice provided by the former NHS Protect. They will also ensure that all of the security work they do will be carried out in a professional and ethical manner.

5.9.2 The Local Security Management Specialists (LSMS) will assist the Trust in providing an environment that is safe and secure so that the highest standards of clinical care can be made available to patients.

5.9.3 The LSMS's also have the following responsibilities:

- to provide advice and guidance to the Trust on security matters and assist the Trust with the creation and development of a pro-security culture
- to undertake investigations into security matters including incidents involving controlled drugs as requested by the Director of Patient Care and Service Transformation
- to ensure that an inclusive approach is taken with regards to security management work involving both internal partners and external partners
- to maintain and collate all reported incidents of security related matters including incidents of verbal aggression and physical assault and provide advice on appropriate actions to be taken to prevent recurrence
- to ensure that the lessons learned from security incidents or breaches inform any further risk analysis and crime prevention work
- to raise awareness of the risks associated with security issues/incidents through campaigns, articles in Staff Matters and possible Hot News bulletins
- to carry out proactive and reactive crime reduction surveys to assess the risk of security breaches in respect of the physical security of premises and assets
- to ensure that all reported physical assault incidents which are notifiable under the Reporting of Injuries, Diseases and Dangerous Occurrences Regulations (RIDDOR) 1995 are reported to the Health and Safety Executive (HSE) within the specified timeframes
- to advise a member of staff who has been assaulted about the appropriate support /counselling that is available to them
- to liaise with external agencies such as the Police, the Crown Prosecution Service to seek sanctions and redress against individuals who either engage in criminal activity against the Trust or who assault Trust employees
- to publicise all sanctions imposed on those who either engage in criminal activity against the Trust or who assault Trust staff
- to assist managers in the completion of risk assessments related to security matters
- to obtain, examine and collate all individual or departmental risk assessments related to security, verbal assault and physical assault that have been carried out within the Trust and identify from them any Trust wide issues.

5.10 Clinical Coordination Centre

5.10.1 The Clinical Coordination Centre will, upon receiving a request from Operational Crews for either operational support or support from the police, endeavour to arrange this support by deploying additional resources and/or requesting police attendance in line with any agreed arrangements. The Clinical Coordination Centre will utilize any agreed escalation process between the Trust and the local police force if police attendance is refused but is deemed necessary by the attending Operational crews.

5.10.2 A central record of vehicle location and equipment is held at each Clinical Coordination Centre (CCC).

5.11 Equipment and Vehicle Review Group

5.11.1 The Trust, via the Equipment and Vehicle Review Group (EVRG), will continually seek to improve the range of equipment supplied to staff.

5.11.2 The EVRG will also review and evaluate all new equipment, including security equipment, purchased by the Trust and ensure that a suitable and sufficient risk assessment on the use and operation of this equipment is carried out.

5.12 Assistant Director of Learning and Development

5.12.1 The Trust's Assistant Director of Learning and Development will be responsible for the implementation and provision of Conflict Resolution Training.

5.13 Estates Department

5.13.1 The Estates Department is responsible for ensuring that all Trust premises have effective and appropriate means of being locked and secured.

5.13.2 The Estates Department is also responsible for the following:

- arranging for the installation, repair and replacement of defective locks (standard locks, digit locks and salto locks)
- issuing of security keys (within their control)
- arrangements for the installation, repair or replacement of signage around Trust premises
- arranging for the repair and replacement of lighting at site (including external lighting and any security lighting within the curtilage of Trust property)
- arranging for the repair or replacement of perimeter fencing around Trust premises
- arranging for the installation of any alarm systems in Trust premises
- arranging for contractors to attend Trust premises.

5.14 Occupational Health

5.14.1 The Occupational Health Department, commissioned by the Trust, have the following responsibilities:

a) to advise the Trust of all aspects of health in the workplace in order to assist the Trust in complying with legal requirements
b) to assess any managers and staff who have been referred to Occupational Health with suspected work-related ill-health and to advise the Trust of the action that should be taken
c) to carry out assessments of medical fitness on staff prior to employment
d) to carry out assessments and advise on the manager or staff member's suitability to return-to-work following an injury sustained at work
e) to provide access to a physiotherapy service. Any member of staff requiring the service is advised to contact the Occupational Health Provider through their line manager

f) to provide a comprehensive rehabilitation programme for staff who have sustained a musculoskeletal injury and meet certain criteria to assist in their recovery to a safe level of fitness so that they can return to work.

6. Definitions

6.1 **Secretary of State's Directions**: These are directions from the Secretary of State to health bodies on measures to deal with violence against NHS staff and on security management measures respectively.

6.2 **Security Management Director** (SMD) is a nominated executive Director with statutory responsibility for overseeing security management work and ensuring compliance with the Secretary of State's Directions. The SMD at the Trust is the Director of Patient Care and Service Transformation.

6.3 **Security breach** is defined as any offence against the Trust, its staff, patients, visitors or contractors. Examples of security breaches may include: physical or nonphysical assaults, theft, criminal damage, unauthorised access to restricted areas or confidential records.

6.4 **Data Protection Act** (DPA) 1998 states the responsibilities of organisations such as the Trust with regard to the processing of personal data and close circuit television systems (CCTV).

6.5 **General Data Protection Regulation 2018** also states the responsibilities of organisations such as the Trust with regards to the controlling and processing of personal data.

6.6 **Physical assault** is defined by the former NHS Protect as: 'the intentional application of force to the person of another, without lawful justification, resulting in physical injury or personal discomfort.'

6.6 **Non-physical assault** is defined by the former NHS Protect as: 'the use of inappropriate words or behaviour causing distress and/or constituting harassment.

7. Suitable and sufficient risk assessments on security

7.1 All identified security matters relating to staff, patients (whilst in the care of the Trust), contractors and visitors (whilst on Trust premises), Trust assets, Medicines and Drugs, Trust property (including information property) and Trust premises shall be subject to the risk assessment process and suitable and sufficient risk assessments using the Trust's generic risk assessment form shall be carried out.

7.2 These suitable and sufficient risk assessments on all identified security matters will be carried out by the appropriate manager with, where necessary, assistance from the Trust's Local Security Management Specialists. This will be done to ensure that the health, safety and security of staff, patients, visitors, Trust assets, Medicines and Drugs, Trust property (including information property) and Trust premises are protected so far as is reasonably practicable.

7.3 The suitable and sufficient risk assessment should identify hazards and the existing controls in place (if any) to protect staff and patients from those hazards and from this evaluate the level of risk. The level of risk should be reduced to the lowest level so far as is reasonably practicable. Therefore, it may be necessary to introduce further measures to manage and control the risks effectively. The significant hazards, risks and controls should be recorded on the risk assessment form.

7.4 When carrying out the suitable and sufficient risk assessments the following, where applicable, should be considered:

- The security of Trust employees, including lone workers and vulnerable workers such as new and expectant Mothers, young persons, students on placement, staff being trained, etc.,
- Potential for verbal and physical assault (although these together with the risk assessment on preventing violence and aggression towards staff are covered specifically in the Trust's Management of violence and aggression policy and procedure).
- Lone working (although this is covered specifically in the Trust's Lone working policy)
- The security of Trust assets and property (including information property)
- The security of Trust premises, buildings and vehicles
- Drugs and medicines management security
- The potential for terrorism.

7.5 The risk assessment should be reviewed periodically to check and ensure that all of the controls that are in place are working effectively.

7.6 The risk assessment should be reviewed and revised following any significant changes to any aspect of the risk assessment. For instance, if there is a change in working practices or changes to the security arrangements in the work place/working environment. All revisions and changes to the risk assessment should be recorded.

8. Crime reduction surveys

8.1 The Local Security Management Specialists (LSMS) will carry out crime reduction surveys of Trust premises to identify the potential for security breaches. The LSMS will also advise and make recommendations to the local manager about addressing any identified security concerns and measures to prevent a reoccurrence of any previous security incident. When carrying out crime reduction surveys the LSMS will use the Home Office's ten principles of crime reduction, see Appendix 2.

8.2 These crime reduction surveys and any associated action plans will be shared with the Health, Safety, Risk and Security Group.

9. NHS Protect Guidance

9.1 In addition to the above, the Trust will consider the guidance of the former NHS Protect and will put measures in place to:

- **deter** criminal activity where possible by putting in place physical barriers such as locks and essential security control systems and procedures to secure Trust property. In addition to other counter measures such as on-going audits and improvements.
- **deny** the criminal any opportunity, not only through physical barriers, but also by putting in place effective systems of observations, loss prevention and property control.
- **detect** the criminal act by carrying out the said risk assessments, crime reduction surveys and audits
- **report** the criminal act by having an incident reporting system in place such as Datix, together with arrangements in place to report the matter to the Police. Staff should report the matter immediately or within 24 hours. The earlier the criminal act is detected and reported, the better the chances of detection and seeking redress.
- **respond** effectively to security issues and problems at all levels with workable counter-measures.
- **Reduce** the reward, such as the marking of Trust property to assist with identification.

Please note, the role of the former NHS Protect has for the time being been taken over by NHS England.

10. Identification badges

10.1 It is the responsibility of employing managers to ensure that all new staff (temporary or permanent) have been issued with an identification badge when they commence employment with the Trust; this badge should be worn in accordance with this policy. If Managers need to obtain an identity badge for their staff card they should send the request to: id.cards@scas.nhs.uk

10.2 It is the responsibility of the line manager to:

- identify what user access level is required by the member of staff and inform the ID Card Team of this
- review the access of staff to Trust premises when they are on suspension, for further information please see advice from Human Resources
- inform the ID Card Team of changes to any access
- ensure that staff return their identity badge when they terminate their employment with the Trust and have it disposed of in an appropriate manner; they should also inform the ID Card Team at: id.cards@scas.nhs.uk

11.Visitor's/Contractor's Identification Badges

11.1 Visitors/contractors should wear their own organisation's identity badges while on Trust property or, if appropriate, be issued with a Trust visitor's badge. Any person who is not known to staff should be challenged and asked for identification provided it is appropriate and safe to do so.

11.2 If a member of staff does not feel it is appropriate or safe to challenge an individual on Trust property that is not known to them should bring the matter to the attention of their manager or a senior officer who may consider further action including contacting the police for assistance.

11.3 If any such person is challenged but is unable to provide identification and a satisfactory explanation (which should be checked) for being on the premises, staff should seek assistance and report the matter to their line manager.

11.4 Line managers or senior officers must take the action appropriate to the situation and circumstances at the time. Their action may for example include escorting the individual from the premises, provided it is safe to do so, or contacting the police.

11.5 Where Trust sites are regularly attended by visitors (e.g. for commercial training purposes) the use of the site by such visitors should be risk assessed and guidelines should be produced. These guidelines should be drawn up taking into account the security of staff, property and information and health and safety considerations. The guidelines should as a minimum refer to the wearing of identity badges/cards, the securing of doors and should define areas where access is restricted or not permitted.

11.6 Visitors should be informed in the guidelines that a breach of these rules may result in expulsion from the training course, without refund of costs.

11.7 All such visitors should be required to sign a copy of the guidelines (to be retained at the site), which should include a declaration that the signatory has read and understood the guidelines and agrees to abide by them.

12. Access to Trust Premises

12.1 It is the intention of the Trust, so far as is practicable, to control access to Trust premises. Employees and visitors are required to wear identification badges in a prominent and visible position on their body at all times whilst on duty/on a Trust premises to:-

- enable staff, patients and visitors to identify legitimate employees
- protect individual employees by enabling then to identify others when handing over keys, other property or materials
- help distinguish between employees, visitors, patients etc.;
- promote greater willingness among employees to challenge people who are not wearing either an identity badge or a visitor's badge whilst on Trust premises or who are acting suspiciously.

13.Smart cards

13.1 Smartcards are issued to operational staff for use with the Electronic Patient Record (EPR) and allow access to the NHS Spine and patient records. The card remains the property of the individual and its use is controlled by a PIN number, which must be kept secure at all times.

13.2 To obtain a smart card, staff need to provide documentation to confirm their address and identity and once this have been verified they will be issued with a smart card and given the appropriate access level as determined by their job role.

13.3 When a member of staff leaves the Trust, it is the responsibility of their manager to check whether the person is going to continue working within the NHS. If they are to continue working in the NHS then the member of staff retains the card to bring with them to their new place of employment. It is the manager's responsibility to advise a Registrations Authority (RA) Agent of this, so that the SCAS profile can be removed from the smart card.

13.4 If, however, the member of staff is leaving the NHS, then the card should be retained by the manager and disposed of in an appropriate manner in accordance with the Registration Authority (RA) guidance. It is the Manager's responsibility to inform the Registration Authority and have them cancel the card on their system.

14. Security of Keys (Access control)

14.1 The Security of keys and levels of access control must be balanced against operational requirements to achieve rapid access and egress in medical emergencies.

14.2 All line managers have overall responsibility for the security of keys for their areas, and that a satisfactory key control process is in place.

14.3 Keys to a Trust building or offices should never be tagged with the name or address of the site/office to which it belongs. Keys to vehicles should not be tagged with the vehicle's registration number. Staff must ensure that buildings are secure when leaving them empty, windows and doors should be locked shut.

14.4 Keys should be kept in locked key cabinets or on an appropriate officer's person.

14.5 If locks are faulty they should be reported as a matter of urgency and where necessary, additional measures implemented to maintain the security of the premises, until the fault has been repaired.

14.6 When a member of staff leaves the Trust or moves to another area within the Trust, line managers should ensure that all keys have been returned prior to his or her departure.

14.7 Digilocks, where used, should be subject to regular combination changes - that is at least once every 6 months.

15.Vehicle security

15.1 The security of Trust vehicles is an issue of paramount importance to the Trust, which recognises the disruption to services and other risks that may be posed as a result of the loss of a Trust vehicle.

15.2 The Trust also recognises that the level of vehicle security must be balanced against operational requirements to achieve rapid access and egress in medical emergencies. Nonetheless, the vehicle should be secured at scene, following a dynamic risk assessment of the scene, location and patient's condition.

15.3 Trust vehicles must be kept as securely as practicably possible. They must not be left in an unsecured area or outside Trust buildings unlocked or with the key in the ignition.

16. Car parking

16.1 Private car parking must be confined to designated areas. Staff must ensure that their vehicles are locked and that all valuables are removed from sight when leaving their private vehicles unattended at Trust sites.

16.2 The Trust will not accept any responsibility for theft from or damage to any private vehicle whilst parked on Trust premises or in the community whilst employees are on official Trust business.

16.3 If any members of staff driving a vehicle of any type on Trust property cause any injury or damage to an individual or property they must report the incident to the Trust and, if necessary, the Police.

17. Intruder alarms

17.1 Staff must ensure that where an alarm is fitted it is correctly set when the building is left unoccupied. Faults and defects in the alarm system must be reported immediately and where necessary, additional measures implemented to maintain the security of persons and premises until the fault/defect has been repaired.

18. Criminal damage

18.1 All incidents of criminal damage and crime must be reported immediately using the Trust's incident reporting system, Datix. The incident must also be reported to the police, LSMS and a unique crime reference number obtained.

18.2 Where criminal damage has resulted in a significant security issue e.g. broken window/damaged door locks appropriate measures must be implemented to maintain security until the damage has been repaired.

19. Signage

19.1 Trust sites are private property. Wherever there is no legitimate reason (such as rights of way) for members of the public to come on to Trust property appropriate signage should be used to deter casual, mischievous, or criminal intrusion (e.g. "NO ENTRY, AUTHORISED STAFF ONLY").

19.2 Such signage should be placed and worded in such a way as to inform visitors and members of the public where access is restricted (both for their own safety and for the security of the site).

19.3 Where CCTV is in operation on Trust sites, the Trust will ensure that there is appropriate and mandatory signage displayed in a highly visible and prominent position at the entry to the site which informs the public that CCTV is in operation.

20. Personal property

20.1 The personal property of an employee is the responsibility of the individual employee and the Trust cannot accept responsibility for its safe-keeping.

20.2 All employees should take appropriate steps to ensure that areas such as offices are secure in order to prevent access by unauthorised persons. Valuable personal property, large amounts of cash etc., should not be brought onto Trust property. If it is then it should be held on the person or stored securely.

20.3 Staff bringing their bicycles onto Trust premises must store them securely in the designated cycle rack. The Trust will not accept any responsibility for the theft or damage of any bicycle that is brought onto Trust premises that is not parked and safely secured in the designated cycle rack.

21. Patient's property

21.1 Whilst a conscious patient is in the care of Trust staff, the patient's property is the responsibility of the said patient; and if the patient is conveyed to hospital then Trust staff may assist with the handing over of the patient's property to staff at the receiving hospital.

21.2 If a member of staff has to look into any purse, wallet and/or bag of a conscious patient then, where possible and practicable, they should seek the permission of the patient beforehand. They should also explain why they are looking into the patient's purse, wallet or bag and 'talk' them through what they are doing.

21.3 If the patient is not conscious or is under the influence of alcohol and/or drugs and does not have the capacity to look after their own property which is being conveyed with them to a receiving hospital then Trust staff will look after this property and hand it over to staff at the receiving hospital.

21.4 If the patient is not conscious or is under the influence of alcohol or drugs and it is not possible to obtain the permission of the patient beforehand then the member of staff should ensure, where possible and practicable, that a chaperone such as a colleague or a police officer is present before they look into the patient's purse, wallet and/or bag.

21.5 Any situation which involves staff looking into a patient's purse, bag and/or wallet must be documented/recorded together with the reasons why such action was necessary; and where possible countersigned by a colleague.

22. Lost and found property

22.1 Any property that is found within Trust premises whose owner cannot immediately be identified and is held to be 'lost and found' property should be handed to either the main reception areas of Trust establishments or to Line Managers.

23. Information technology security/Smart Cards

23.1 This policy does not encompass security relating to information technology and information systems. Details of the arrangements the Trust has in place for information technology security can be found in the Trust's Corporate ICT Security Policy.

24. Security of controlled drugs

24.1 Detailed guidance on the security of controlled drugs can be found in the Trust Controlled Drugs Policy.

25. Cooperation with NHS England (Including Counter Fraud)

25.1 The Trust must co-operate with the NHS England (including Counter Fraud) to enable the NHS England to efficiently and effectively carry out its functions in relation to security management. In particular the Trust will:

a) Enable representatives of NHS England to have access to its premises;

b) Put in place arrangements which enable NHS England to interview, as appropriate, its staff for the purpose of carrying out its security management functions as soon as it is reasonably practicable and in any event within seven days from the date the request was made;

c) Supply such information including files and other data (whether in electronic or manual form) as NHS England may require for the purpose of carrying out its security management functions as soon as is reasonably practicable subject to NHS and Trust confidentiality rules.

25.2 The Trust will respond to a request from NHS England as soon as is reasonably practicable and in any event within seven days from the date the request was made.

26. Training

26.1 Managers and staff will receive training in accordance with the Trust's training needs analysis and its statutory and mandatory training programme.

26.2 Managers and Supervisors who have to carry out risk assessments on manual handling tasks must obtain training in how to do so from the Risk Team prior to undertaking any risk assessments as per this policy.

27. Equality and Diversity

27.1 An equality and diversity impact assessment has been carried out on this policy and can be found at appendix 4.

28. Monitoring

This policy will be reviewed as indicated on the front sheet – or sooner subject to legislative change.

28.1 The effectiveness of this policy will be monitored in the following way.

29. Consultation and Review

29.1 A consultation exercise on the policy will be carried out with the relevant stakeholders

29.2 This policy will be reviewed every three years or sooner if there are any relevant changes to legislation or best practice.

30. Implementation (including raising awareness)

30.1 The policy will be implemented and communicated to managers and staff within the Trust via the weekly newsletter, Staff Matters. Emails will also be sent to senior managers and area managers asking them to bring the existence of the policy to their staff.

31. References

- Health and Safety at Work Etc. Act 1974
- Secretary of State's Directions for Security Management 2003/2004 (Amended 2006)
- Secretary of State's Directions to health bodies on measures to deal with violence against NHS staff
- Management of Health Safety at Work Regulations 1992 (Amended 1999)
- Workplace Health, Safety and Welfare Regulations 1992
- Provision and Use of Work Equipment Regulations 1992 (Amended 1998)
- Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995.
- Children's Act 1989 Police Act 1997 part V
- Safeguarding legislation
- Private Security Act 2001
- Crime and Disorder Act 1998
- Regulation of Investigatory Powers Act 2000
- The Telecommunications (Lawful Business Practice) Interception of Communications Regulations 2000
- Data Protection Act 1998
- General Data Protection Regulation 2018

32. Associated documentation

- Health and safety policy
- Management of violence and aggression policy and procedure
- Lone working policy

- Close Circuit Television (CCTV) policy
- Medicines management policy
- Controlled drugs policy
- Dignity at work policy
- Whistleblowing policy
- Safeguarding policy
- Adverse incident reporting policy
- Reporting of Injuries, diseases and dangerous occurrences regulations (RIDDOR) policy
- Risk management strategy

33. Appendix 1: Review Table

A full review has been carried out for this policy. A review table is available on request.

34. Appendix 2: Principles of Crime Reduction

1. The ten principles of crime reduction are:

1.1 Target hardening is making targets more resistant to attack or more difficult to remove or damage. A target is anything an offender would want to steal or damage; it could be an object, property or person.

1.2 Examples of target hardening may include:

- Fitting better doors or windows;
- Fitting window or door locks;
- Installing alarms;
- Repairing damaged or derelict property

2. Target removal

2.1 Target removal is the permanent or temporary removal of vulnerable persons, vehicles or property. This means making sure that any object in which a potential offender might be interested in is not visible. This can include:

- Removing radios from parked;
- Placing valuable items in a secure location;
- Making property less visible from the outside.

3. Remove the means to commit crime

3.1 Removing the means to commit crime is making sure that material capable of being used to help an offender commit a crime is not accessible. This can include:

- Moving bins away from windows;
- Locking up equipment after use;
- Securing building materials such as scaffolding.

4. Reduce the payoff

4.1 Reducing the payoff means reducing the gain or reward for the criminal if a crime is committed. This can include:

- Security tagging or marking items to make them identifiable.

5. Access control

5.1 Access control means restricting access to sites, buildings or parts of sites or buildings. This can include:

- Door locks;
- Identity cards;
- Entry card systems;
- Keypad entry systems.

6. Visibility/Surveillance

6.1 This principle means making sure that offenders would be visible if they carried out a crime. This can include:

- Pruning or removing shrubbery;
- Improving or installing lighting;
- Changing the height of fences;
- Installing alarm systems;
- Installing CCTV systems;
- Neighbourhood watch schemes.

7. Environmental Design

7.1 Environmental design involves changing the environment of a building or site to reduce the opportunities to commit a crime. This can include many of the features specified within this appendix including:

- Visibility/surveillance;
- Target hardening;
- Lighting;
- Path/walkway layout

8. Rule setting

8.1 Rule setting means the introduction of policies, procedures or codes of conduct which set out what is acceptable behaviour. This can include:

- Wearing identity badges;
- Signs prohibiting access by unauthorised persons;
- Requests to report to reception;
- Internal rules.

9. Increase the chances of being caught

9.1 This means introducing anything that slows down the offender or increases their risk of being caught. This can include:

- Proper management of surveillance arrangements;
- Lighting that makes offenders more visible;
- Alerting offenders to the fact that surveillance arrangements are in place;
- Publicising successes in detecting offenders.

10. Deflecting Offenders

10.1 Deflecting offenders means diverting the offenders and potential offenders from committing crime. This can include:

- Education programmes and campaigns;
- Attending youth groups and organisations.

It should be noted that not all principles will be applicable for all scenarios. Further advice and guidance can be obtained from the Trust's Risk and Security Manager.

35. Appendix 3: Responsibility Matrix – Policies, Procedures and Strategies

The responsibility for this policy is shared between various Policy Groups, Lead Director/Officers, Working Groups and Committee members.

A full list of all responsible parties can be made available upon request.

36. Appendix 4: Equality Impact Assessment Form Section One – Screening

Employees exercising their rights and entitlements under the regulations will suffer no detriment as a result.

The Screening element of the ‘Equality Impact Assessment’ is available on request.

37. Appendix 5: Equality Impact Assessment Form Section Two – Full Assessment

Employees exercising their rights and entitlements under the regulations will suffer no detriment as a result.

A full ‘Equality Impact Assessment’ is available on request.

38. Appendix 6: Ratification Checklist

Policy Title	Security Policy
Author's Name and Job Title	John Dunn, Head of Risk and Security
Review Deadline	
Consultation From – To (dates)	4/3/2016 to 25/3/2016; 16/1/2019 to 23/1/2019.
Comments Received? (Y/N)	Y
All Comments Incorporated? (Y/N)	Y
If No, please list comments not included along with reasons	

Equality Impact Assessment completed (date)	31/12/2015; 16/1/2019.
Name of Accountable Group	Health, Safety and Risk Group
Date of Submission for Ratification	

Template Policy Used (Y/N)	Y
All Sections Completed (Y/N)	Y
Monitoring Section Completed (Y/N)	Y
Date of Ratification	20/5/2016; 23/1/2019
Date Policy is Active	20/5/2016; 23/1/2019
Date Next Review Due	20/5/2019: January 2022

Signature of Accountable Group Chair (or Deputy)
Name of Accountable Group
Chair (or Deputy) Chief Operations Officer.