South East Coast Ambulance Service NHS
NHS Foundation Trust

Security Management Policy

Contents

1. Statement of Aims and Objectives

1.1. South East Coast Ambulance Service NHS Trust (the Trust) is committed to ensuring, as far as is reasonably practicable, the health, safety and welfare of employees, including contractors and volunteers; of patients, their families and carers; and of those affected by Trust actions. This document aligns to the NHS Violence Reduction Standards, South East Coast Ambulance Violence Prevention and Reduction strategy and procedural documents. The trust takes a public health, trauma informed approach to supporting staff affected by violence or aggression.

1.2. The overriding principle of this policy is to detail the provisions, and requirements to enable security management to provide associated specialist services for the Trust, to protect staff and assets from criminality and to deliver a secure service for those who operate for the Trust and for the people we serve. Through development of systems and processes, the Trust will provide suitable security arrangements as far as practicably possible, to work towards this principle.

1.3. The Policy will also detail the responsibilities of management and staff for their security, their colleagues' security, and the people we serve.

1.4. In the event an incident could not be avoided, for any security related incident, such as violence and aggression, theft, criminal damage etc. the Trust, where possible, will pursue sanction and redress.

1.5. Security of operatives for the Trust is particularly emphasised in relation to those likely to be exposed to incidents of physical and non-physical assault. It is recognised that this is not exclusive to front line operational staff, but could affect anyone such as delivery drivers, receptionists and those working in the Call Handling Centres (EOCs / 111) who may be the victim of verbal abuse and aggression.

1.6. The Trust recognises its obligations to the security of staff in line with the Assaults on Emergency Workers (Offences) Act 2018, Investigatory Powers Act 2016 along with supporting operatives as the victims of criminal offences by those external of the Trust. Legislation is underpinned by the NHS National Violence Reduction Standard to support the work for the security of operatives, patients and Trust assets.

1.7. **Security of Assets:** The Trust also strives to ensure that Trust assets of all types are kept secure and the potential for theft or criminal damage is minimised. In today's society, vehicles, equipment, and premises are vulnerable in respect of damage and theft, any of which could result in loss or irreparable damage or loss of function, and in turn this could have an impact on service provision.

1.8. The Security Services have also highlighted the national risk from terrorist activities, in particular the use by such organisations of ambulance

vehicles as a Vehicle Borne Improvised Explosive Device or as means to avert suspicion through disguise as legitimate vehicle or legitimate personnel, and that protection of assets is related to prevention of such circumstances. In addition, a significant amount of the Trust's annual budget is spent on the physical assets of the organisation i.e., vehicles, equipment, and Trust estate.

1.9. This policy applies to all staff employed by the Trust, including temporary / agency staff, Trust contractors and volunteers.

2. Principles

2.1. The Trust follows the Secretary of State's Directions issued to Health bodies and will manage security issues via the Nursing and Quality Executive Director and the Security team.

2.2. The Executive Director will lead at Senior Leadership level and the Security team outside of this as the senior role on these issues, however it is a responsibility of all employees of the Trust to assist in the effective management of security.

2.3. **Violence and Aggression Procedure.**

2.3.1. **Education and Training**: All staff as part of their key skills training will receive conflict resolution training via the online workbooks on ESR each year, conflict is on a 3-year cycle. "NHS|CSTF|NHS Conflict Resolution (England) - 3 Years".

2.3.2. **History Marking**: To reduce the possibility of staff incidents the Trust will maintain a database of addresses ("History Markers") within the Emergency Operations Centre (EOC), of persons who have previously subjected operatives of the Trust to violence and/or aggression. In the event of further calls to this person, attending staff will be advised of the previous behaviour of the subject to assist them in judging the situation and how to proceed. In more serious cases, the crew may determine to rendezvous with the Police prior to an attendance.

2.3.3. **Dynamic Risk Assessment**: Dynamic Risk Assessments are the basis that Trust operatives must use to make informed decisions for entering or removing themselves from any substantiated and credible threats. They should also utilise any available information the Trust holds, such as overarching risk assessments, local or Trust wide, History Marking, Security Alerts etc. where the information is directly applicable to the call or attendance at the time.

2.3.4. In all cases, the balance of the duty of care to patients must be matched with the priority of ensuring the safety of Trust operatives; however, this duty of care requires that, in the provision of emergency treatment,

reasonable steps should be taken to ensure that the public are not put unnecessarily at risk and that their needs should also be considered.

2.3.5. **Summoning Assistance**: All Operational Staff, whether part of a crew or acting as lone workers must have a means of raising assistance or calling for help.

2.3.6. **Within the Trust this will be via:**


Fixed telephone


Fixed panic button


Mobile telephone


Radio

2.3.7. It is recognised that whilst these devices will not prevent incidents occurring, they do provide a means of calling for assistance and obtaining aid; to minimise the severity of incidents.

2.4. **Management of incidents of violence, aggression and abuse.**

2.4.1. All incidents of violence and aggression must be reported via the Trust's incident reporting system.

2.4.2. The Security Team must be notified via the reporting system of the incident to allow contact to be made with the operative where appropriate to offer advice and support on subsequent steps that can be taken both locally and criminally.

2.4.3. Where an incident of violence and aggression has occurred, the Trust advocates strongly that the matter is reported to the police as a crime, however the decision to do so is ultimately the victim's own.

2.4.4. The Security Team, on behalf of the Trust, where required can support and assist with all police investigations into incidents of violence and abuse against Trust staff and follow up on each case as it progresses, until such time it is concluded.

2.4.5. Information gained on the outcome from cases should be shared with the victim in the first instance by Security Management.

2.5. **Prevention of Theft and Criminal Damage.**

2.5.1. The Trust will maintain, as far is reasonably practicable, a secure environment for the safekeeping of information, staff and patient property and equipment, vehicles, property, and other assets of the Trust.

2.5.2. Premises security Any employee entering Trust premises that is not their usual place of work, or where their presence is not recorded by the use of the Trust access control system, must sign a register noting the date and time of their visit.

2.5.3. Any visitor to premises used by the Trust who is not displaying a Trust identity pass must be signed into the building and given a visitors pass.

2.5.4. The Trust must encourage staff to challenge those not displaying either a Trust or visitors pass, where safe to do so, asking them to identify themselves and the purpose of their visit.

2.5.5. Whilst stations are unoccupied, all external doors and windows capable of allowing entry to a person and garage shutter doors must be securely closed. Staff should be mindful that many thefts are opportunistic, and the likelihood should be reduced by closing garage and internal doors, and ensuring windows are not left open.

2.5.6. **Door codes**: The majority of Trust premises have swipe access but where numeric door codes are in use as means for access control, these shall be changed in the following circumstances:

- In response to a security incident at a location.
- Where there are ground to believe the codes have been compromised.
- As part of a scheduled door code change facilitated by Estates.

2.6. Investigatory Powers Act (IPA)

2.6.1. The IPA, formerly the Regulatory Powers Act (RIPA), provides law enforcement agencies and security services across the country with provisions for ‘serious crime’ detection investigations and powers that may supersede an individual’s privacy rights.

2.6.2. The Trust is responsible for having a Senior Responsible Officer (SRO), which would be the senior post for security.

2.6.3. Any investigation which may impact on privacy rights of another must be referred to the SRO/Trust Lead for Security for review and approval.

2.6.4. In such cases where an IPA investigation is suitable, the Trust’s Lead for Security is also the Single Point of Contact (SPOC) who liaises with the Home Office to submit the application.

2.7. **Security of Personal Property**.

2.7.1. All staff are responsible for their own private property, including storage and safe keeping.

2.7.2. The Trust is responsible for providing all staff with a means of secure storage, for staff to safely store personal items and clothing.

2.7.3. Staff are advised not to unnecessarily bring personal items (particularly valuables) onto Trust property.

2.7.4. The Trust will not be responsible for the loss of or damage to staff private property brought onto site, including their personal vehicle or personal items within a Trust vehicle.

2.8. **Medicines, Drugs and Gases.**

2.8.1. Wherever these are stored on Trust property, they will be kept securely in accordance with the Trust's Medicines Management Policy and in line with the legal requirements for the storage of drugs (controlled or otherwise).

2.8.2. The Security of medicines, drugs and gases on Trust sites and response vehicles is an essential responsibility of all operatives and the management for the site and operating area.

2.8.3. Any discrepancy in the drugs register will be reported by staff to their line manager and an incident report form (IWR-1) completed in line with the applicable policy and will prompt an immediate audit to confirm the shortfall.

2.8.4. Where there is a shortfall, the Trust shall investigate at a level appropriate to the nature and extent of the loss, including but not limited to Local Management, the Police, Counter Fraud Investigation, and investigation by the Security team.

2.9. Any issues of broken or otherwise unusable drugs shall also be accounted for via an incident report form (IWR-1).

2.10. **Vehicle security**

2.10.1. Whenever vehicles used by Trust operatives are left unattended on or off a Trust site, ALL doors and windows must be locked where reasonably practicable to do so.

2.10.2. It is recognised that vehicle security must be balanced with service provision, so as to allow a swift activation in the case of an emergency response, though should not be relied on where it is clear time was available to shut and/or lock a door using the remote on the keys. However, vehicles not responding or involved in Trust business that is time critical must be secured when unattended.

2.11. Patient's Property

2.11.1. Staff should care for any property a patient brings onto the vehicle and should assist in ensuring it is transferred to where the patient is to receive treatment.

2.11.2. Patients should, wherever possible, be advised not to carry an excessive amount of property or valuables (i.e., jewellery, expensive items, or large amounts of money).

2.11.3. The Trust will investigate all items reported as lost or missing by patients through its Patient Experience Team (PET).

2.12. Identification Cards

2.12.1. All SECAmb staff must have a means to identify themselves as legitimate Trust employees.

2.12.2. Operatives must carry their Identification (ID) Cards on their person at all times whilst on Trust business, as a means to confirm their identity.

2.12.3. Lost and stolen ID cards shall be reported via the Trust's incident reporting processes, following immediate contact with Security Management to ensure all access rights are cancelled and to prevent any unauthorised access.

2.12.4. ID cards must not, under any circumstances, be used (either for access or identification) by any other person than the person named on the card.

2.12.5. Dishonest/inappropriate use of ID cards and/or failure to report a lost ID card with access permissions would be deemed as a Trust security breach. Where deemed intentional, reckless or negligent, this could be subject to disciplinary proceedings being invoked under the Trust Disciplinary Policy.

3. Management of incidents of theft or criminal damage.

3.1. Incident reporting

3.1.1. All incidents of theft and/or criminal damage, where either confirmed or suspected, must be reported via the Trust's incident reporting system.

3.1.2. Security Management must be notified at the earliest opportunity of the incident to allow contact to be made with the employee/manager to offer appropriate instructions on subsequent remedial steps that must be taken.

3.1.3. Where a crime has taken place, or is suspected to have taken place, the Security Team will instruct the appropriate person (usually the responsible

Manager, or person most knowledgeable of the incident) to contact the police and report the incident (See 2.6.2.3) for the exceptions when an employee is implicated).

3.2. Internal thefts/damage/security issues

3.2.1. The Trust recognises that, with over 4500 operatives, there is a likelihood of criminal activities taking place within the Trust workforce that are perpetrated by Trust operatives.

3.2.2. These must be addressed in a robust consistent manner, however, should be done in conjunction with Human Resources and following the Disciplinary Policy, as well as Police involvement.

3.2.3. Unlike incidents of criminality perpetrated by external persons to the Trust, which would always be reported to the police, where an employee is involved it would be *usual* for the police to be involved; but the Trust may make the decision not to do so based on the nature and extent of the incident, as well as any other factor, and may instead choose to refer the matter to internal disciplinary proceedings either prior to, or instead of, police involvement.

3.2.4. **Bag Searches:** The Trust does not have the contractual right to search employees' belongings without their permission, but may engage with employees, or the police, where a search is deemed necessary by written permission of a Silver Officer, as highlighted by the Security Management Procedure.

3.3. Security Audits

3.3.1. The Trust will have a Security Audit conducted where the site is considered of a critical nature, a serious risk has been identified or an incident/breach of security has been identified. These will consider;

- Updating within at least three years of the last report.
- Any major or persistent security issue at that site.
- Any structural change to the site itself, or new site becoming operational.

3.4. Lockdown Requirements

3.4.1. The Trust has a requirement to undertake a lockdown risk profile for each of its organisational sites and other specific buildings/areas (such as Emergency Dispatch Centres or Make Ready Centre).

3.4.2. The profile will consider the many aspects that are central to this theme as part of the Crime Reduction survey performed for each site (i.e. surrounding area/buildings, security of external doors, key control etc.)

3.4.3. These individual assessments, once completed for each site within the Trust, shall be compiled into an organisational overview, highlighting specific and general areas of concern, with recommendations and subsequent Trust wide instructions for the lockdown process.

3.4.4. The Trust must be prepared to implement these lockdown procedures where necessary to secure an organisational site against a threat and have prepared business continuity plans to ensure the continuance of service provision.

3.4.5. It is recognised that the Trust estate covers numerous buildings across three counties. As such the deadline for completion is in line with those for the Security Audits above.

3.5. Deterrence and Promotion of Security Issues

3.5.1. The Trust will publicise externally the unacceptability of violence and abuse against employees of the Trust with a view to making would-be offender's aware that violent and aggressive behaviour will not be tolerated, and where deliberate will result in criminal sanctions.

3.5.2. The Trust will use internal means to highlight recent achievements and successes to staff concerning convictions and sanctions achieved for any type of criminality concerning the Trust.

3.5.3. The Trust will also use internal means to publicise security issues and encourage security mindedness through the use of reminders relating to issues and concerns that have been raised.

4. Definitions

Assets:	Within the Trust and the wider NHS, the terms "property", "assets" and "equipment" are used interchangeably to describe NHS owned items, vehicles and estate. For the sake of clarity in this policy, the terms above will relate to: Trust buildings (owned and/or leased) Trust vehicles of all types. Fixtures, fittings and furniture within buildings and vehicles. Medical and non-medical equipment of all types. Consumables and supplies of all types procured by the Trust. NHS equipment that is personally issued. Any other item that the Trust has procured.

	Staff personal items and belongings are not considered Trust assets, however these are recognised as being items which the Trust should facilitate security measures for, where reasonably practicable, without bearing responsibility for their loss or damage
Security Incident	Any occasion where an operative is subjected to threatening behaviour whilst operating for the Trust, verbal abuse or physical assault or a situation where Trust assets are stolen, damaged or otherwise compromised in a manner not authorised by the Trust.
Theft	The dishonest appropriation of property belonging to another with the intention of permanently depriving the other of it.
Criminal Damage	When any individual, without lawful excuse, destroys or damages property belonging to another, intending to destroy or damage such property or being reckless as to whether such property is destroyed or damaged.
Physical Assault	The intentional application of force to the person of another, without lawful justification, resulting in physical injury or personal discomfort.
Non-Physical Assault	The use of inappropriate words or behaviour causing distress and / or constituting harassment.
Dynamic Risk Assessment	For the purposes of this document and the focus on protection against violence, defined as the continuous assessment of risk and safety in relation to changes in the environment and gathered information in relation to potential threats; used as a basis for deciding the safety of entering, remaining or withdrawing from the environment.

5. Responsibilities

5.1. Chief Executive Officer

5.1.1. Ultimately Responsible for all policies and procedures within the Trust, including those relating to the reduction of violence and aggression to Trust staff and ensuring suitable redress is pursued.

5.2. The Trust Board

5.2.1. The Trust Board is responsible for ensuring that the Violence Prevention and Reduction Strategy is implement and tracking progress of its delivery.

5.2.2. **Executive Director Nursing and Quality**: Responsible for promoting security at Board level, and for monitoring and ensuring compliance with the requirements and directions issued by the Secretary of State, the Department of Health and NHS England relating to security.

5.2.3. **Directors**: Responsible for ensuring that the principles and guidelines issued to assist in preventing and detecting incidents of violence and abuse,

or those for enhancing the security of Trust or private property are implemented by their directorates.

5.3. **Security Team**

5.3.1. Responsible for assisting the Trust to realise the requirements and directions issued by the Secretary of State, Department of Health and NHS England relating to security.

5.3.2. Responsible for escalating to the SMD awareness of security issues which may affect the Trust, its staff, patients or the levels of service.

5.3.3. Develop and lead on Trust wide improvement plans for Security Management and have oversight of assurance work to ensure a strong security culture is embedded.

5.3.4. Is the named role in charge of Security for the Trust's Controlled Drugs Licence.

5.3.5. Is the named role as the SRO under IPA for investigations detecting crime where the offence would constitute "serious crime."

5.3.6. To advise on crime reduction measurements of Trust properties and activities which may place employees, patients and the public at risk.

5.3.7. To provide specialist expert information, guidance and training to assist directors, managers and staff in the performance of tasks and duties in relation to Security Management.

5.3.8. Oversee the investigation of security incidents in accordance with established practice and legislation and liaise with the Police, NHS England and other relevant parties to secure suitable sanction where necessary.

5.3.9. Liaise with the Police, Crown Prosecution Service (CPS), NHS England and other interested stakeholders and act on their behalf as required in the best interests of the Trust, and where required in an effort to secure prosecutions, give evidence or otherwise to safeguard the Trust, and its activities.

5.3.10. Act where required as the official Trust Witness to support cases through the Criminal Justice System for security related incidents affecting the Trust.

5.3.11. Is the Trust's representative/member at the National Ambulance Violence Security Group (NAVSEG)meetings and supports the determination of best practice for local Trust implementation.

5.3.12. The Trust Lead for Security will liaise with the Trust's Local Counter Fraud Specialist (LCFS) where security issues are raised that are of joint or mutual

interest, or where specialist advice or assistance is needed. An MOU is in place for this.

5.3.13. Responsible for administration of Security Incidents on the Trust's Incident Reporting System and ensuring managers conduct proportionate security related investigations.

5.3.14. Responsible for the administration of the Trust's ID card system.

5.3.15. Circulating advice set out by specialists/management/senior management, to support violence, aggression, theft, criminal damage cases etc. as well as processes around ID card management, CCTV, BWC and lone working.

5.4. Managers and Team Leaders

5.4.1. Responsible for ensuring that those under their supervision comply with the principles and guidelines issued to assist in preventing and detecting incidents of violence and abuse, or those for enhancing the security of Trust or private property.

5.4.2. Responsible for ensuring that all incidents are reported, that they complete an appropriate internal investigation, and they ensure adequate support is given to the victim of the crime.

5.5. All Employees

5.5.1. Responsible for reporting all security incidents in which they are the victim (i.e. they have been abused, assaulted or had property stolen) or to which they become aware (e.g. theft of or damage to property).

5.5.2. Responsible for co-operating with the principles and guidelines issued to assist in preventing and detecting incidents of violence and abuse, or those for enhancing the security of Trust or private property.

5.5.3. Must make dynamic risk assessments for all incidents to which they respond, to assess the potential for danger or injury to themselves and balance their obligations to providing emergency healthcare with the safety of themselves, patients, or other members of the public.

5.6. Competence

5.6.1. The Trust will ensure that they employ a competent person, who holds suitable qualifications and experience for Security, able to provide leadership for Security Management for the Trust.

6. Monitoring

6.1. Information is available to all staff in personal security and how to report incidents of criminality; in addition, frontline operational staff receive conflict resolution training, which is refreshed on a three yearly basis as part of their annual key skills training.

6.2. All incidents of criminality, violence and abuse will be recorded on the Trust's incident reporting system by the Trust's Security Team. These will be investigated by the appropriate Manager and will be monitored for completion by the Security Team.

6.3. Trend analysis information pertaining to incidents of violence are reported to the following groups;

- Medicines Governance Group (which Security is a standing member of).
- Medical Gasses Group (which Security is a standing member of).
- History Marking Working Group (which Security is a standing member of).
- Health and Safety Working Group.
- Quality and Patient Safety Committee (QPS)
- Integrated Performance Report (IPR Dashboard)

6.4. The figures are provided as part of the Key Performance Indicators document, denoting the number of incidents, as well as comparisons per 100 staff and per 1000 ambulance responses made by the Trust.

6.5. The Trust Board receives statistical information on a bi-monthly basis, relating to instances of violence and aggression.

6.6. The Trust Board has agreed to tolerances for all Dashboard information where an Exception Report would be required to account for any significant changes in these figures.

6.7. The Trust Risk Register must reflect the risk of violence and abuse against staff and be reflective of on-going prevention and management. The risk must be graded appropriately to reflect the consequence and likelihood of such incidents and must be reviewed on a two monthly basis prior to each meeting of the QPS.

6.8. All History Marks shall be monitored, audited and updated by the History Marking Review Group, which meets on a monthly basis, of which the Security Team is a standing member.

7. Audit and Review

7.1. The Lead role for Security will ensure that they are cognisant of the contents of this policy; continuously reviewing the content through its use, to ensure it meets the security needs of the Trust, whilst remaining relevant and appropriate prior to its scheduled review.

7.2. All policies have their effectiveness audited by the responsible Management Group at regular intervals, and initially six months after a new policy is approved and disseminated.

7.3. Effectiveness will be reviewed using the tools set out in the Trust's Policy and Procedure for the Development and Management of Trust Policies and Procedures (also known as the Policy on Policies).

7.4. This document will be reviewed in its entirety every three years or sooner if new legislation, codes of practice or national standards are introduced, or if feedback from employees indicates that the policy is not working effectively.

7.5. All changes made to this policy will go through the governance route for development and approval as set out in the Policy on Policies.

8. Equality Analysis

8.1. The Trust believes in fairness and equality, and values diversity in its role as both a provider of services and as an employer. The Trust aims to provide accessible services that respect the needs of each individual and exclude no-one. It is committed to comply with the Human Rights Act and to meeting the Equality Act 2010, which identifies the following nine protected characteristics: Age, Disability, Race, Religion and Belief, Gender Reassignment, Sexual Orientation, Sex, Marriage and Civil Partnership and Pregnancy and Maternity.

8.2. Compliance with the Public Sector Equality Duty: If a contractor carries out functions of a public nature then for the duration of the contract, the contractor or supplier would itself be considered a public authority and have the duty to comply with the equalities duties when carrying out those functions.

9. References

- Health Care Act 1977
- Assaults on Emergency Workers (Offences) Act 2018
- Investigatory Powers Act 2016
- Offences Against a Person Act 1861
- Theft Act 1968
- Criminal Damage Act 1971
- Criminal Justice Act 1988
- Protection from Harassment Act 1997
- Malicious Communications Act 1988
- Communications Act 2003
- NHS Violence Prevention and Reduction Standard
- The Department of Health and Counter Fraud Strategy:2020-2023
- Health and Safety at Work Act (1974)