Proud to care in Sheffield

NHS
Sheffield Health
and Social Care
NHS Foundation Trust

Policy:

FIN 008 Security

Executive Director lead	Executive Director of Operations & Transformation
Policy owner	Security Officer
Policy author	Security Officer

Document type	Policy
Document version number	Version 9
Date of approval by PGG	29/08/2023
Date of ratification	14/09/2023
Ratified by	Quality Assurance Committee
Date of issue	September 2023
Date for review	September 2026

Summary of Policy
This policy provides the governance structure and duties required of the to minimise security incidents throughout all activities provided by or on behalf of Sheffield Health and Social Care NHS Foundation Trust (SHSC).

Target audience	All SHSC staff and the Trust Board

Keywords	Security, safety, duty of care, assault, violence

Storage

Version 9 of this policy is stored and available through the Sheffield Health and Social Health NHS Foundation Trust's, (SHSC), intranet and internet.

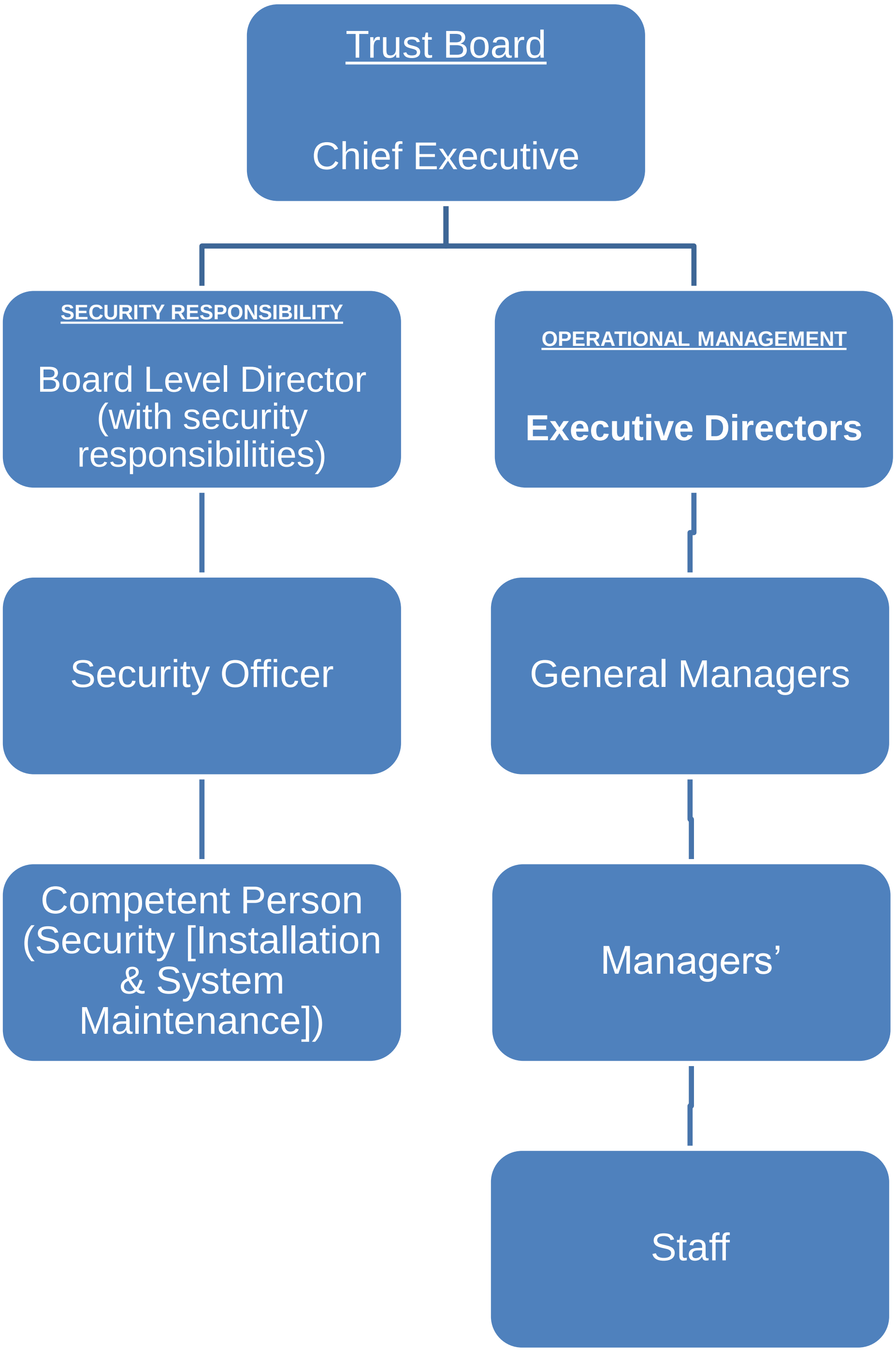
This version of the policy supersedes the previous version, (V8: November 2021).
All copies of the previous policy held separately should be destroyed and replaced with this version.

Version Control and Amendment Log

Version No.	Type of Change	Date	Description of change(s)
8	Review on expiry of policy	August 2021	New policy commissioned by EDG on approval of a Case for Need.
9	Review	October 2022	Early review undertaken to update the policy to in order to include revised Duties and Procedures requirements.
9	Review	August 2023	Policy provided to Policy Governance Group for approval, minor changes requested to Executive Director Lead and other contents.

Contents

Security Flowchart:



1. Introduction

Sheffield Health and Social Care NHS Foundation Trust (SHSC) recognises its responsibilities under Health and Safety legislation to ensure so far as is reasonably practicable the health, safety and welfare of its employees, service users and any relevant persons for whom it holds a duty of care.

Security is often described as the protection from, or the resilience against, potential harm caused by others, by restraining the freedom of others to act. Effective security provision depends on a combination of physical measures and robust systems of effective management. Security safety within a healthcare environment is particularly challenging due to the complexities of healthcare services and the provision of access within premises to staff, service users and visitors.

Whilst physical security measures within a building are intended to provide protection to building occupants, effective security management ensures that incidents of security breaches resulting in individual injury or harm, unauthorised access and egress, theft, vandalism, damage and assault etc... are minimised so as to prevent the disruption in the provision of healthcare services in a safe and secure environment.

It is important that staff take responsibility for their actions to minimise the likelihood of a security incident from occurring.

2. Scope

This policy applies to:

- All premises and property owned or leased by SHSC.
- Staff employed by SHSC, (full-time and part-time employees).
- Visitors, contractors, and persons engaged in business on behalf of SHSC.

3. Purpose

SHSC seeks to provide a safe environment for staff, patients and visitors by providing security measures across sites, training to deal with violence and aggression and to minimise security risk to all through continuous vigilance and improvement.

4. Definitions

An explanation of terms used within this policy is provided below:

- **Physical assault** - the intentional application of force to a person without lawful justification, resulting in physical injury or personal discomfort.

- **Non-physical assault** - the use of inappropriate word(s) or behaviour causing distress and/or constituting harassment.

- **Work-related violence** - (Health and Safety Executive (HSE) definition) - any incident in which a person is abused, threatened or assaulted in circumstances relating to their work.

- **Theft** - dishonestly appropriates property belonging to another with the intention of permanently depriving the other of it.

5. Details

The details and requirements of this policy are applicable to all members of staff, contract staff and volunteers employed by or engaged in activities on behalf of SHSC.

6. Duties, Roles and Responsibilities

SHSC through its governance structure, will ensure appropriate risk mitigation measures are identified and implemented to minimise incidents and occurrences which are considered to pose a significant risk to effective delivery of healthcare service provision.

6.1 Trust Board

The Trust Board has overall accountability for security management throughout SHSC providing appropriate levels of investment in the estate and personnel to facilitate the implementation of suitable security measure to provide a safe and secure environment.

The Trust Board will facilitate the development of partnership initiatives with stakeholders and other appropriate bodies in the provision of security arrangements where reasonably practicable.

The Trust Board will discharge the responsibility for security management through the Chief Executive.

6.2 Chief Executive

The Chief Executive on behalf of the Trust Board will ensure that all arrangements for the provision of care and other services by third parties include sufficient contractual arrangements to ensure compliance with SHSC policy requirements.

The Chief Executive will discharge the day-to-day operational responsibility for security management through the Director with security management responsibility.

6.3 Board Level Director (with security responsibility)

The Director of Strategy will be the Board Level Director (with security responsibilities) who is responsible for ensuring security issues are highlighted at Board Level, this responsibility will extend to the proposal of programmes of work related to security management for consideration as part of the business planning process including security-management components of the capital programme and future allocation of funding.

The Board Level Director will assist the Chief Executive ensuring that security systems and arrangements are suitable to minimise the occurrence of security incidents likely to affect the efficient delivery of healthcare services. The Director will appoint a suitable qualified person to provide advice and assistance to help deliver an environment for those who use and work within SHSC which is safe and secure.

6.4 Security Officer

A suitably trained Security Officer will support the Board Level Director (with security management responsibilities) in the provision of advice to prevent, deter and detect security incidents with regard to building security systems to minimise the occurrence of security incidents. Where specialist solutions are required to resolve security issues, the Security Officer would not necessarily be expected to have the level of skill required but would know the limits of their capabilities and, when necessary, seek the advice from a specialist third party.

6.5 Local Management

Directors of Service, Heads of Service, General Managers, Departmental Managers, Team Leaders, and Clinical Leads have delegated responsibility to ensure that suitable and sufficient security arrangements are devised and implemented to protect assets, property, staff and persons for which a duty of care is held providing a safe and secure environment to minimise the likelihood of security incidents occurring that effect the operational delivery of healthcare services.

Managers are responsible for the monitoring of security arrangements and provisions within areas for which they have delegated responsibility ensuring that contraventions of security measures are reported in accordance with SHSC policy: *Incident Management (Including Serious Incidents) Policy* and Procedure (MD 023).

Managers are to ensure that local security risk assessments are undertaken, maintained up-to-date and managed in accordance with SHSC Document: *Risk Management Strategy* ensuring:

- risk assessments are in place and where significant security risks exist local controls are in place mitigate risk to as low as is reasonably practicable,

- staff are briefed with regard to their own personal security and local procedures, where appropriate,

- all staff are issued with staff identification badges,

- work areas under their control are operated in accordance with this policy and any associated procedures,

- all breaches of security arrangements are investigated and reported immediately in accordance with incident reporting policy and procedures,

- faults with Trust security systems are reported to Estates without delay,

- all staff upon leaving the organisation return their staff identification badges, uniforms, organisation issued keys, electronic passes and any issued security alarm system or personal protective equipment,

- confidential records are secured in line with Trust policy,

- advice is sought, as appropriate, where there is any doubt as to the standards that are to be applied in adhering to this policy,

- response is made at the earliest opportunity to any request from employees for advice on security concerns,

- all security incidents are recorded using the Trust incident reporting system.

Managers are to undertake an internal audit of workplace security arrangements to ensure they remain ‘fit for purpose’. Managers must maintain appropriate records of workplace safe systems of work, procedural arrangements, risk assessments and demonstrate staff awareness of the policy, which should be reviewed annually, or as considered appropriate.

6.6 Staff, Contract Staff and Volunteers

All staff, contractors and volunteers are required to comply with any SHSC security requirements as devised to provide a safe and secure environment, report deficiencies in security arrangements to line managers and always ensuring the promotion of safe and secure practices to help reduce the occurrence of security incidents.

All employees have a duty to co-operate with the implementation of this policy, staff should ensure:

- they bring to the attention of their immediate manager, or duty manager, as appropriate, any suspicious activity they observe on the organisation’s premises,

- they report all incidents of violence and aggression at the earliest opportunity,

- they adhere to all relevant departmental local procedures and make use of systems provided in identified areas,

- they wear their staff identification badges at all times when on duty (where safe to do so),

- they bring to the attention of their line manager any perceived shortcoming or failings in security arrangements,

- they make full and proper use of personal lockers (if available) and take all reasonable care for their own property whilst at work,

- they report immediately to their departmental manager any loss, or malicious damage to, their own, patients or Trust property,

- that faults with Trust hard fixed security systems are reported to Estates without delay,

- where issued with personal safety alarms or other personal protective equipment is accounted for, remains fully operational and returned at the end of their shift or other continuous period of work.

7. Procedure

Managers are to devise and implement appropriate procedural arrangements to mitigate and minimise the occurrence of security incidents within areas for which they have devolved responsibility.

General Security Arrangements

Departmental managers have responsibility for the securing their own departments and ensuring advice and local procedures are in place to manage security risk. All services, teams and wards must have a current security risk assessment. All premises shall be suitably secured to prevent unauthorised access during and outside of normal working hours or when core services are closed. Where sites are shared with other services local procedural arrangements are to be put in place to ensure collective responsibility for security. Advice from the Security and Fire Officer should be sought on the adequacy of local security arrangements where considered necessary.

Access Control

Service managers at all Trust premises are to ensure that there are local written procedures detailing measures governing access to areas under their control. They should coordinate with service mangers in adjacent areas of the same building to ensure that security in these areas is not compromised.

It is particularly important that access is only granted to those who have a requirement to be in a particular area; therefore, access to staff-only, clinical, and other restricted areas, must be appropriately controlled.

Electronic Access Control Cards are provided by the Estates Department upon receipt of a request from a line manager, where electronic access control systems are installed, they must be appropriately managed with access fobs or cards only issued as part of a formal process which balances the operational needs of the service with the protection of Trust property and the health and safety of employees, contractors, patients and other legitimate visitors. Managers are to ensure that access cards and fobs are obtained in accordance with the local procedure for sites and are removed from members of staff when they no longer have a requirement for them, or access restrictions have been enforced.

Automated access control systems allow the use of fobs, cards or other tokens to release door locks electronically. Such systems are managed like networked computer systems and should be subject to the following administrative rules:

- no access control card, fob or token should be issued unless specifically authorised by an appropriate manager,

- managers should ensure that access control permissions are removed from staff when they leave or move to another team. Access control should be team and role specific and re-authorisation should occur when that role changes,

- access control permissions should also be removed if an employee will not be using the access control system for some time. If an employee is on maternity leave or long-term sick leave but will be returning to work, then access may be retained. If an employee is on detachment for a significant time, is suspended for disciplinary reasons or is still employed but not expected to return to work then access rights should be removed.

7.1 Risk Management

All managers are required to comply with the requirements of SHSC Document: *Risk Management Strategy: Responsibilities and accountabilities for risk management Section 31* to make risk management a fundamental part of their approach to clinical and corporate governance responsibilities. They are to ensure that an assessment of risks relating to security of staff, visitors and assets are undertaken in accordance with the Risk Management Strategy.

7.2 Incident Reporting

SHSC utilises the electronic Ulysses Risk Management System to facilitate the reporting of incidents. All staff have a responsibility to ensure security incidents are reported on Ulysses to allow management to investigate and review the causes of the incident and development remedial actions to minimise reoccurrence so far as reasonably practicable.

All reported incidents including near misses must be reported before the end of the working day or working shift in which the incident occurred/became known.

7.3 Management of Aggression and Violence

SHSC acknowledges that staff, service users and visitors may be exposed to or involved directly in incidents of aggression or violence, SHSC Policy: NP 030 *Use of Force Policy – Prevention and Management of the Use of Force Safe and positive care,* provides guidance to statute, procedure and best practice in relation to the conflict resolution, prevention and use of force.

Incidents of aggression and violence involving members of the public are not to be tolerated and must be reported to the Police, incidents involving service users will be investigated and assessed on an individual basis to determine whether Police assistance is required.

SHSC will provide suitable conflict resolution training known as ‘RESPECT’ to staff in the management of conflict directed towards them from service users. The training aims to identify potential situations likely to lead to conflict allowing staff to implement de-escalation techniques to minimise aggression and violence.

7.4 **Security and Management of Assets and Property**

SHSC will through its governance structure provide suitable resources as considered appropriate to ensure, assets and property are suitably protected by means of physical, psychological and all other security measures to minimise the likelihood of damage or loss. All staff are to ensure suitable and sufficient arrangements are implemented to protect assets and property for which they have delegated responsibility.

Line Managers are to ensure that new members of staff receive local induction of the security arrangements appertaining to their area of work the team and their role. See SHSC Policy: *Induction Policy (HR 009), Appendix B – Induction Checklist – Health and Safety.*

SHSC will ensure, through its governance arrangements, that its assets and belongings, and those of service users for which it has responsibility, are suitably protected to prevent damage or loss from inappropriate actions or criminal activity.

7.5 **Investigations, Sanctions and Publication**

All staff are to report incidents/offences committed against staff or organisational assets and property for investigation. Where considered appropriate following a review of an Incident, the Incident Investigation Officer may seek assistance from the Security Officer and/or the Police.

Incidents committed by members of the public are to be reported both on the Ulysses Incident Reporting System and to the Police, staff reporting the incident to the Police are to ensure a Police Incident Number or Crime Reference Number is obtained and included on the Ulysses Incident Report.

SHSC will, where considered appropriate undertake sanctions against individuals committing offences against SHSC staff, service users, assets and property and consider publicising sanctions in appropriate media with a view to deterring other potential offenders.

7.6 **Recovering Financial Losses**

SHSC will endeavour to recover any financial losses as a result of theft, damage to assets, property or premises etc. caused by criminal activity.

All such losses are to be reported by line management in submitting the relevant report forms in accordance with SHSC Policy: *Incident Management Policy and Procedure (including Serious Incidents)* and the SHSC Policy: *Losses and Special Payments* Policy (FIN 013).

7.7 **Major Incident and Contingencies – Lockdown**

In the event of a major incident the SHSC Policy: *Emergency Preparedness, Resilience and Response (EPRR) Policy (OPS 005)* outlines how the organisation will operate during a major incident. In the event the control of movement is required within a premise, a process known as lockdown will be implemented.

Lockdown is the controlling of movement, access, and egress of people from around or into an area or premise in response to an identified risk, threat or hazard that might impact upon the security of staff, service users or visitors.

7.8 **Medicines, Drugs, Prescription Forms and Hazardous Materials**
SHSC will ensure all medicines are strictly controlled. Specific instructions to assist staff in the control and management of medicines are available in SHSC Policy: *Medicines Optimisation Policy Risks and Processes (MD 013).* Members of staff who are accountable and responsible for medicines, drugs and prescription forms are to be familiar with the policy requirements and implement identified security arrangements devised for medicine security.

7.9 **Counter-terrorism**
All staff should be constantly vigilant for the threat of terrorist activity. Terrorist activities range from overt acts, such as shootings, bombings and chemical attacks; they also take more subtle forms such as information gathering and blackmail.

Staff should be aware of suspect packages, un-attended items, the threat of bomb attacks and suspicious incidents, which are to be reported immediately to their line manager, building manager and the Trust's Security and Fire Officer.

External advice from security specialists, including the Counter-Terrorism Security Advisor (CTSA), employed by South Yorkshire Police will be consulted as considered necessary to ensure the provision of protective and counter-terrorism measures are appropriate to the threat(s) posed to the Trust.

Improvised Explosive Devices (IEDs), Chemical, Biological and Radiological and Nuclear (CBRN) devices are often delivered in a variety of forms and could be considered as a suspicious package or object. Staff should be particularly aware of items, objects or devices which:

- should not be there,
- cannot be accounted for,
- are out of place with its surroundings.

Where it is suspected that an IED has been identified, under no circumstances are members of staff to attempt to open it/them.

7.10 **Lone Working**
SHSC recognises that some members of staff will at times, be required to work on their own or away from their base location to undertake part of their duties. Effective managerial arrangements must be implemented to ensure, so far as reasonably practicable, the security and wellbeing of lone workers in accordance with SHSC Policy: *Lone Worker Policy (HR 042).*

7.11 **Dangerous and 'Offensive' Weapons**
The term 'weapon' means any knife, or other type of sharply bladed or pointed object, or any object that could be used to threaten or injure another person. Any implement or object which could cause injury or harm may be

considered to be a ‘dangerous’ weapon, e.g., a chair, screwdriver or other similar objects. The carrying of such an object is not an offence; however, when brandished in a threatening manner it is an ‘offensive’ weapon. All such incidents involving offensive weapons are to be reported to the Police. ‘Offensive’ weapons are redefined within the *Prevention of Crime Act (1953)* as ***‘any article made or adapted for the use for causing injury to the person or intended by the person having it with him for such use by him or by some other person’**.*

Any weapon brought into SHSC premises by a service user(s) should be confiscated, placed in a secure located, the Security Officer is to be informed who will make arrangements for its collection and disposal via the Police.

It is acknowledged that some service users, (i.e. Sikhs), wish to carry a Kirpan, a ceremonial knife, as an act of religious obligation. After plenty of discussion and consideration it has been decided that it is un-acceptable for this to occur on SHSC premises.

All items referred to as Kirpans will be treated in the same way as any other potentially dangerous or offensive weapon, as described above.

Some Kirpans are made of materials so as not to be categorised as dangerous or offensive weapons to allow the person to meet their religious obligation. In such circumstances, and upon assessment by the Police, the Kirpan will be retained in safe keeping until the service user leaves Trust premises and it is appropriate to return the item to them.

SHSC will place the wellbeing of all its service users above that of any one individual, and the carrying of a ‘harmless’ Kirpan has the potential to confuse service users and the public as to the Trust’s position on knives. It may even cause distress to a service user whose perception is altered due to confusion, or due to persecutory or paranoid ideation.

7.12 Closed Circuit Television (CCTV) Surveillance Systems

CCTV is often used as an aid to enhance observation or surveillance of identified areas as a risk mitigation control measure, where such systems are designed to capture and record data images reference should be made to SHSC Policy: *Recording Policy (IMST 010).*

7.13 Car Parking and Vehicle Security

SHSC provides car parking facilities at many of its premises, SHSC does not accept any liability or responsibility for damage caused to private vehicles parking in its car parks, vehicle owners park their vehicles at their own risk.

Vehicle Owners are responsible for the security of their private vehicles and for ensuring they fully comply with any Terms and Conditions for parking within sites where car parking management and enforcement applies.

7.14 **Lost and Found Property**
All lost and found property must be investigated and reported in accordance with SHSC Policy: *Handling Lost and Found Property* (FIN 012).

7.15 **Door Access Control**
Door access control measures will be provided where considered appropriate to restrict access to identified areas, Local Management Teams are to consider the type of access control restriction that may be required to address identified risks. Door access control measures include the use of physical keys and locks, digital keypads and electronic keypads utilising smart card/device technology.

8. Development, Consultation and Approval

Name of Policy: **Security**	**Name of Policy Lead**: **Stephen Price**
Date: **October 2022**	**Contact Details**: **(0114) 271 8189**
Consultation Plan: This policy is applicable to all SHSC staff, volunteers and contractors. The policy will be provided to: Board Level Director (with security responsibilities), Service Directors, Health and Safety Manager, Ward Managers, Unison Members and placed on the SHSC Intranet Policy Forum - Policy consultation page to allow comments and amendments to be provided prior to being submitted for approval and ratification.	

RECORD OF CONSULTATION (interactive)

Group or individual consulted	**Date of consultation/ response received**	**Comments on draft policy**	**Your response (say if policy amended - if not, why not)**
Director of Strategy	28/03/2023	Nil	
Service Directors	18/10/2022	Nil	
Health and Safety Manager	18/10/2022	Changes to draft text and inclusion of additional text	Policy amended to reflect changes
Ward Managers	18/10/2022	Nil	
Unison Members	18/10/2022	Nil	
SHSC Intranet Forum – policy consultation	18/10/2022	Nil	

Health and Safety Committee	23/05/2023	Nil	
Policy Governance Group	29/08/2023	Minor changes to Executive Director Lead and Contents	Implemented
Executive Director of Operations & Transformation	30/08/2023	Executive name change	Implemented

9. Audit, Monitoring and Review

Monitoring Compliance Template

Minimum requirement	Process for monitoring	Responsible individual/ group/committee	Frequency of monitoring	Review of results process (e.g. who does this?)	Responsible individual/group/ committee for action plan development	Responsible individual/group/ committee for action plan monitoring and implementation
Policy monitoring	Levels of reported incidents	Incident Huddle	Daily	Clinical Quality and Safety Group	Quality and Assurance Committee	Quality and Assurance Committee
Policy Monitoring	Levels of reported incidents	Health & Safety Committee	Monthly	Quality and Assurance Committee	Quality and Assurance Committee	Quality and Assurance Committee

10. Implementation Plan

Action/Task	Responsible Person	Deadline	Progress update
The draft, revised policy submitted to identified individuals and groups for consultation	Security Officer	September 2022	Policy distributed for consultation
Comments received for consideration and amendment	Security Officer	November 2022	Comments received and policy amended
Policy sent to the Health and Safety Committee for approval	Security Officer	April 2023	Policy submitted for approval
Health and Safety Committee submit Policy to the Policy Governance Group	Security Officer	May 2023	Policy approved by HSC 23.05.2023
The Policy Governance Group approve the policy and submit it to the Quality Assurance Committee for ratification	Chair of Policy Governance Group	TBC	
Policy sent to the Quality Assurance Committee for ratification	Chair of Policy Governance Group		
Policy placed on the Trust's intranet and internet for dissemination. All previous versions to be removed with an email alert to all staff	Policy Governance Group		
Managers to inform staff for which they have responsibility of the revised Policy	Managers		

11. Dissemination, Storage and Archiving (Control)

Upon ratification of this policy, an ‘All SHSC staff’ email alert will be sent to staff, informing them of the new/revised policy and attaching the link showing where the policy can be accessed via the intranet and internet. Directors of Service are to ensure all teams and areas are made aware of this new/revised policy and how to apply it.

The previous Security Policy will be removed from the Trust intranet by the Director of Corporate Governance and archived on the policy database. Team managers are responsible for ensuring it is also removed from any policy and procedure manuals, or files stored in their offices, and destroyed.

12. Training and Other Resource Implications

Security Awareness Training is to be an integral part of organisational training and education in accordance with the Trust’s *Risk Management Strategy.*

SHSC will provide suitable conflict resolution training known as ‘RESPECT’ to staff in the management of conflict directed towards them from service users, Line managers are to undertake a staff training needs analysis and consider the type of training required, all staff are required to undertake RESPECT training on an annual basis.

13. Links to Other Policies, Standards, References, Legislation and National Guidance

- Crime Prevention Act (1953)
- Department of Health’s (DH) document: A Professional Approach to Managing Security in the NHS.
- NHS Protect: Tackling crime against the NHS – A strategic approach.
- NHS England: Violence prevention and reduction standard (2020)
- SHSC policy: *Incident Management (Including Serious Incidents) Policy* and Procedure (MD 023.
- SHSC Document: *Risk Management Strategy.*
- SHSC Policy: MD 023 -*Incident Management Policy and Procedure (including Serious Incidents*).
- SHSC Policy: NP 030 *Use of Force Policy – Prevention and Management of the Use of Force Safe and positive care*.
- SHSC Policy: *Incident Management Policy and Procedure (including Serious Incidents)* and the SHSC Policy: *Losses and Special Payments* Policy (FIN 013).
- SHSC Policy: *Induction Policy (HR 009).*
- SHSC Policy: Emergency Preparedness, Resilience and Response (EPRR) Policy (OPS 005).
- SHSC Policy: *Medicines Optimisation Policy Risks and Processes (MD 13).*
- SHSC Policy: *Lone Worker Policy (HR 042).*
- SHSC Policy: *Recording Policy (IMST 010).*
- SHSC Policy: *Handling Lost and Found Property (*FIN 012).

14. **Contact Details**

Title	Name	Phone	Email
Executive Director of Operations & Transformation	Neil Robertson	2718747	Neil.robertson@shsc.nhs.uk
Security Officer	Stephen Price	2718189	Stephen.price@shsc.nhs.uk

Appendix 1
Equality Impact Assessment Process and Record for Written Policies

Stage 1: **Relevance** - is the policy potentially relevant to equality i.e. will this policy potentially impact on staff, patients or the public? This should be considered as part of the Case of Need for new policies.

NO - no further action is required; please sign and date the following statement.

I confirm that this policy does not impact on staff, patients or the public.
Name/Date: Stephen Price, April 2023

YES, go to **Stage 2**

Stage 2: Policy Screening and Drafting Policy - public authorities are legally required to have 'due regard' to eliminating discrimination, advancing equal opportunity and fostering good relations in relation to people who share certain 'protected characteristics' and those that do not. The following table should be used to consider this and inform changes to the policy (indicate yes/no/ don't know and note reasons). Please see the SHSC Guidance and Flow Chart.

Stage 3: Policy Revision - make amendments to the policy or identify any remedial action required and record any action planned in the policy implementation plan section.

SCREENING RECORD	Does any aspect of this policy or potentially discriminate against this group?	Can equality of opportunity for this group be improved through this policy or changes to this policy?	Can this policy be amended so that it works to enhance relations between people in this group and people not in this group?
Age	**No**	**No**	**No**
Disability	**No**	**No**	**No**
Gender Reassignment	**No**	**No**	**No**
Pregnancy and Maternity	**No**	**No**	**No**
Race	**No**	**No**	**No**
Religion or Belief	**No**	**No**	**No**
Sex	**No**	**No**	**No**
Sexual Orientation	**No**	**No**	**No**
Marriage or Civil Partnership	**No**		

Policy Amended:

Impact Assessment completed by Stephen Price, April 2023

Appendix 2

Review Policy Checklist

This checklist to be used as part of the development or review of a policy and presented to the Policy Governance Group (PGG) with the revised policy.

		Tick to confirm
	Engagement	
1.	Is the Executive Lead sighted on the development/review of the policy?	✓
2.	Is the local Policy Champion member sighted on the development/review of the policy?	✓
	Development and Consultation	
3.	If the policy is a new policy, has the development of the policy been approved through the Case for Need approval process?	N/A
4.	Is there evidence of consultation with all relevant services, partners and other relevant bodies?	✓
5.	Has the policy been discussed and agreed by the local governance groups?	✓
6.	Have any relevant recommendations from Internal Audit, or other relevant bodies, been taken into account in preparing the policy?	✓
	Template Compliance	
7.	Has the version control/storage section been updated?	✓
8.	Is the policy title clear and unambiguous?	✓
9.	Is the policy in Arial font 12?	✓
10.	Have page numbers been inserted?	✓
11.	Has the policy been quality checked for spelling errors, links, accuracy?	✓
	Policy Content	
12.	Is the purpose of the policy clear?	✓
13.	Does the policy comply with requirements of the CQC or other relevant bodies? (where appropriate)	✓
14.	Does the policy reflect changes as a result of lessons identified from incidents, complaints, near misses, etc.?	✓
15.	Where appropriate, does the policy contain a list of definitions of terms used?	✓
16.	Does the policy include any references to other associated policies and key documents?	✓
17.	Has the EIA Form been completed (Appendix 1)?	✓
	Dissemination, Implementation, Review and Audit Compliance	
18.	Does the dissemination plan identify how the policy will be implemented?	✓
19.	Does the dissemination plan include the necessary training/support to ensure compliance?	✓
20.	Is there a plan to: i. review ii. audit compliance with the document	✓
21.	Is the review date identified, and is it appropriate and justifiable?	✓