Policy:
FIN 008 Security

Executive Director lead	Director of Special Projects (Strategy)
Policy owner	Security and Fire Officer
Policy author	Security and Fire Officer

Document type	Policy
Document version number	Version 8
Date of approval by PGG	25/10/2021
Date of ratification	10/11/2021
Ratified by	Quality Assurance Committee
Date of issue	November 2021
Date for review	December 2024

Summary of Policy

This Policy outlines the expectations of the Trust Board for employees of the Trust to discharge their duties as befits their position to minimise and address the risks which jeopardise the security of staff, service users, assets, and the environment for which it holds a duty of care.

If you have any concerns about the content of this document, please contact the author.

Target audience	All SHSC staff and the Trust Board

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

Storage

Version 8 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, (V7: October 2018).
All copies of the previous policy held separately should be destroyed and replaced with this version.

Contents

Version Control and Amendment Log

Version No.	Type of Change	Date	Description of Change(s)
7	Review on expiry of policy	July 2018	Amendments to Sections 5 (*Duties*) and 6 (*Processes).* Removal of attached procedural instructions, namely: • Security Assessment Check Sheet • Tackling Violence and Anti-Social Behaviour • Lockdown • Improvised Explosive Devices (IEDs) and Similar Threats • Offensive Weapons 6.5 - *Reporting Incidents and Serious Untoward Incidents* changed to *Reporting Incidents and Serious Incidents*.

8	Review on expiry of policy	August 2021	*Flow Chart*: amended
			Contents: amended
			Section 3 *Purpose*: Inserted - Private Accommodation
			Section 6 *Duties of Trust Board*:
			     Security Management Director (SMD): removed
			     Director of Finance: removed
			     Director of Special Projects (Strategy): inserted

Flowchart:

Section 1: Introduction

The Trust Board commits to minimise the impact of such occurrence on personal safety, the delivery of patient care, the environment and property.

Section 2: Scope

The Trust Board indicates who this policy is applicable to.

Section 3: Purpose

The Trust Board provides an unambiguous statement of intent to minimise the occurrence of security incidents.

Section 6: Duties

The Trust Board indicates its intention to discharge its responsibilities as a provider of healthcare to ensure that suitable and sufficient governance arrangements are in place to manage security-related matters directing staff devise and implement appropriate arrangements as befits their duties.

Section 7: Procedure

Operational Managers implement the policy, develop risk assessments and arrangements, seeking specialist advice where appropriate to minimise or mitigate identified risks.

1.   **Introduction**

This document explains the strategic approach Sheffield Health and Social Care NHS Foundation Trust, (SHSC), will take to provide a safe and secure physical environment that has suitable systems and arrangements in place to protect staff from violence, harassment and abuse, safeguard property and assets from theft, misappropriation or criminal damage.

The Trust will deliver a security strategy designed to meet the aims of the document through its governance structure by addressing the priority areas:

- **Creating a pro-security culture**
  The Trust will, through its governance structure, allow for the creation of a pro-security culture whereby staff are supported and encouraged to effectively manage security arrangements within their workplace and report any security incidents, including theft, un-authorised access, violence and other unacceptable practices when they occur.

  The Trust will provide Security Awareness Training to all staff during corporate and local workplace induction. Line managers will explain security systems and arrangements applicable to members of staff and the support systems available as required.

- **Deterrence**
  The Trust will implement appropriate, protective measures including physical and psychological barriers to deter or delay criminal activities. The purpose of deterrence methods is to convince potential attackers that a successful attack is unlikely due to strong, external and internal defences.

  Physical measures to protect work premises, including walls, fencing, intrusion detection systems, restricted access points, warning notices, lighting and Closed-Circuit Television (CCTV) surveillance will be considered by the Trust as a safety control measure.

- **Preventing**
  The Trust will develop appropriate procedural arrangements to prevent security incidents or breaches from occurring in the first instance, or minimise the risk of them occurring, learning from operational experience and shared best practice. Employees and authorised persons will be provided with suitable means of identification, i.e. identity cards which will require to either be displayed or be in their immediate possession for inspection as necessary as a deterrent to prevent avoidable breaches in security provisions.

- **Detecting**
  All Trust premises will be provided with suitable electronic and/or physical security systems to detect breaches in security provisions. Staff are required to be vigilant and conscious of persons acting suspiciously within Trust premises and not displaying approved personal identification. They are to report any incident immediately to their line manager, an alternative senior member of staff or the Police, (if deemed appropriate).

- **Investigating**

  All breaches in security are to be investigated by line management in accordance with the Trust's governance arrangements.

  Investigations are to be undertaken in a fair, objective and professional manner to ensure those responsible for such incidents are held to account for their actions. Where it is considered that redress is required to be taken against individuals responsible for causing, injury, harm, fear or damage to staff, service users or organisational assets, support and assistance is available from the Trust's Security Officer and Police.

Increased Security Threats

Following the identification of an increased security threat, additional resources may be allocated to mitigate, where considered appropriate. Where it is considered that a security service is required, which cannot be provided internally by staff, approved external contractors will be appointed. All external, security contractors will to be commissioned via the Facilities Directorate.

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
   - Sub-contractors
   - Students
   - Volunteers
   - All other persons engaged in business on behalf of SHSC.

   Responsibility for the management of this policy will be devolved in accordance with the organisation's devolved management structure, which includes aspects of crime prevention. The responsibility of operational managers is to ensure procedural arrangements within their sphere of responsibility are devised and implemented, taking account of security issues and that staff groups for which they have responsibility receive appropriate training.

   The day-to-day management of security issues will remain the responsibility of operational managers. SHSC will appoint a Security Officer who will act in an advisory capacity to support staff to enable them to discharge their responsibilities.

   The Trust, through its governance structure, will ensure appropriate risk mitigation measures are identified and implemented to protect, detect and respond to incidents and occurrences which are considered to pose a significant risk to effective service provision.

3.   **Purpose**

To provide an unambiguous statement of intent to minimise the occurrence of security incidents applicable to the Trust and to premises where healthcare treatment on behalf of the Trust is delivered or received, excluding private accommodation.

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.

Duty of care - (Health and Safety at Work Act (1974) Section 7) - it shall be the duty of every employee whilst at work:

- To take reasonable care for the health and safety of his/herself and other persons who may be affected by his/her acts or omissions at work.

- As regards any duty or requirement imposed on her/his employer, or any other person, by or under any of the relevant statutory provisions, to co-operate with him/her, so far as is necessary, to enable that duty or requirement to be performed or complied with.

5.   **Detail of the Policy**

The broad overview of this policy is provided in the Introduction.

6.   **Duties**

The **Trust Board** will:
- Discharge its responsibilities as a provider of healthcare to ensure that suitable and sufficient governance arrangements are in place to manage security-related matters.

- Provide appropriate levels of investment in the estate and personnel to facilitate the implementation of suitable security safety precautions.

- Facilitate the development of partnership initiatives with stakeholders and other appropriate bodies in the provision of security arrangements where reasonably practicable.

Implementation:
The Trust Board expects those tasked with managing aspects of security within areas for which they are accountable and have devolved responsibility to:

- Diligently discharge their duties and responsibilities as befits their position.

- Have in place a clearly defined management structure for the delivery, control and monitoring of security arrangements.

- Have in place a programme for the assessment and review of workplace risks.

- Develop and implement appropriate protocols, procedures and control measures to assist in the mitigation of security risks.

- Develop and disseminate appropriate management plans pertinent to each building/department/area to ensure the safety of occupants, protect the delivery of service and, as reasonably practicable, protect the property and environment.

- Develop and implement monitoring mechanisms to address reported security incidents.

Executive Directors
The Executive Directors are responsible for ensuring the operational delivery of the Trust's strategic direction.

Scheme of Delegation
The Trust may make such arrangements, as considered appropriate, to ensure its functions are implemented by a committee, sub-committee, the Chair, a director or by an officer of the Trust; in each case subject to such restrictions and conditions as the Board deems suitable in accordance with the Trust's Scheme of Delegation Policy.

Chief Executive
The Chief Executive is accountable for security within SHSC and will appoint, where necessary, an appropriate Executive Director with responsibility for security management.

Director of Special Projects (Strategy)
The Director of Special Projects (Strategy) is responsible for the health, safety and welfare of Trust employees and persons for whom a duty of care is held.

Security Officer
The Security Officer is responsible for the provision of specialist security advice and assistance in matters of security within the workplace to mitigate identified risks.

Head of Procurement
The Head of Procurement will ensure all purchases are made in accordance with the Trust's document: *Standing Orders, Reservations and Delegation of Powers and Standing Financial Instructions.*

Accountable Emergency Officer

An Executive Director will be appointed as the Trust's Accountable Emergency Officer who, with support from the Emergency Planning Manager, is responsible for ensuring the Trust has suitable arrangements devised in response to a major incident and that detailed guidance on actions to be undertaken in such circumstances is contained within the policy *Emergency Preparedness, Resilience and Response (EPRR).*

Executive Director of People

The Executive Director of People is responsible for ensuring security-related issues are addressed within the SHSC personnel policies and implementation of the government's 'PREVENT' programme, which aims to support, protect and safeguard the Trust's staff and service users.

Chief Pharmacist

The Chief Pharmacist is responsible for medicines management throughout the Trust, including effective governance and security arrangements for the safe management of medicines. The Chief Pharmacist Associate is the Trust's 'Accountable Officer for Controlled Drugs' and is responsible for the assurance of governance relating to controlled drugs.

Heads of Service

Heads of Service are responsible for ensuring suitable governance arrangements are brought to the attention of staff and implemented within all areas where they have devolved responsibility. Where it is considered necessary, safety arrangements should be implemented to protect staff working alone within private accommodation in accordance with Policy HR 042 - Lone Worker.

Director of Facilities Management

The Director of Facilities Management is responsible for the development of secure facilities as directed by the Trust Board and for devolving responsibility to appropriate persons to plan, design and maintain the security of Trust premises.

Head of Estate Services

The Head of Estate Services is responsible for ensuring appropriate advice, technical support and control measures are provided by suitably-qualified persons for the monitoring, installation and maintenance of security measures within Trust premises.

Head of Capital and Strategic Development

The Head of Capital and Strategic Development is responsible for ensuring a secure environment is considered at the briefing, planning, design and construction stages of all new-build or refurbishment projects using a risk-based approach.

Managers

Managers with devolved responsibilities are to ensure all reasonable and practical measures are undertaken to identify, evaluate and mitigate security risks.

Staff

All staff have a responsibility to comply with authorised instructions and management arrangements, which have been devised to provide a safe and secure environment.

7. **Procedure**

The following processes have been devised to mitigate risk, where appropriate.

7.1 **Identifying Risks**
The person(s) delegated with responsibility for workplace activities must manage the health and safety of staff, and other relevant persons for whom they have responsibility, in accordance with the *Health and Safety at Work Act 1974.*

In addition, they must undertake workplace risk assessments and record significant risks in accordance with the *Management of Health and Safety at Work Regulations 1999* and the Trust's *Health and Safety* Policy.

The Trust has a *Risk Management Strategy,* which describes the processes for effectively managing risks within the Trust.

Potential hazards and risks likely to affect security management - especially those health and safety risks that may pose a significant risk to staff, (e.g., physical assault), service users and other relevant persons - are to be reported in accordance with the Trust's risk management strategy.

Specialist advice should be sought, where applicable, regarding the identification of appropriate control measures to address and mitigate safety risks.

7.2 **Assessing Risks**
Workplace risk assessments are to be undertaken and managed in accordance with the Trust's *Risk Management Strategy* and supporting documents*.*

7.3 **Risk Management and Action Plans**
Workplace risk assessments and action plans devised to mitigate risk are to be made readily available, upon request by any relevant person(s).

Where deemed appropriate, crime prevention partnerships - with an interest in security within the NHS - will be established with external organisations, including the Police and other agencies.

7.4 **Risk Review**
A review of the control measures identified within a risk assessment is to be undertaken following reported incidents, or changes to workplace processes, with a view to ensure they remain suitable and sufficient to mitigate identified risks, so far as reasonably possible.

7.5 **Reporting Incidents and Serious Incidents**
The Trust has specific incident reporting arrangements. All security breaches and incidents, as documented throughout this policy, should be reported in accordance with the Trust's *Incident Management Policy and Procedure (including Serious Incidents*). All staff should to be aware of and familiar with incident reporting arrangements.

7.6 Protection of Staff - Tackling Aggression and Violence

The Trust acknowledges that staff may be exposed to or involved directly in incidents of aggression or violence while providing healthcare services. Incidents involving members of the public are not to be tolerated and must be reported to the Police while incidents involving service users will be investigated and assessed on an individual basis. Information on the management of aggression and violence is provided in the Trust's policy *Aggression and Violence Policy (NP 030 V4 December 2020).*

In order to make a full assessment of whether an individual accused of offending should be arrested, charged or diverted from the criminal justice system, the Police are to be provided by the Trust with appropriate information on mentally vulnerable suspects to assist them in determining an appropriate course of action.

The Trust will undertake a training needs analysis to identify staff roles and responsibilities and provide suitable Conflict Resolution Training (CRT) to effectively manage potential incidents of workplace violence and aggression.

7.7 Security and Management of Assets and Property

The Trust will ensure that all staff, assets and property are suitably protected by means of physical, psychological and all other security measures as considered appropriate to achieve an identified aim. Responsibility for the security of staff, assets and property will be delegated to managers and staff in accordance with the Trust's policy document: *Scheme of Delegation.*

Managers with responsibility for work premises are to devise, record and bring to the attention of relevant staff any security arrangements with the purpose of providing a safe and secure environment.

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

The Director of Finance will, in accordance with the *Scheme of Delegation,* delegate powers to manage the approval of financial transactions initiated by other directorates across the Trust, prepare, document and maintain detailed financial procedures and systems incorporating the principles of separation of duties and internal checks to supplement instructions.

Directors of Service, other directors and line managers have delegated responsibility to ensure all reasonable measures are undertaken to protect and secure the organisation's assets and property to prevent loss and/or damage.

Organisational assets valued in excess of £5,000 will be recorded on a Corporate Asset Register. Departmental business critical assets valued below £5,000 will be recorded and held on a central register with suitable procedural arrangements developed to ensure the lifecycle of the asset is monitored from procurement to return, decommissioning and disposal.

7.8 **Investigations, Sanctions and Publication**
The Trust will investigate all reported incidents/offences committed against staff or organisational assets. The Investigation Officer will, where considered necessary, seek assistance from the Trust's Security Officer and/or the Police. Incidents committed by members of the public are to be directed to the Police for investigation.

The Trust will, where sanctions are taken against individuals, consider publicising sanctions in appropriate media with a view to deterring other potential offenders.

All staff have a 'duty of care' in accordance with the Trust's policy document: *Scheme of Delegation* to protect staff, Trust assets and property from the point of procurement to disposal. Managers are to devise suitable procedural arrangements, where considered necessary, to ensure assets are accounted for and property, for which they have responsibility, are appropriately secured and protected. Measures to deter, prevent and detect criminal activities are identified in Section 9.1 *Strategy*.

7.9 **Recovering Financial Losses**
The Trust 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 Trust policy document: *Incident Management Policy and Procedure (including Serious Incidents)* and the policy document: *Losses and Special Payments* to Directorate Nominees.

7.10 **Major Incident and Contingencies - Lockdown**
In the event of a major incident the Trust will implement its policy document: *Emergency Preparedness, Resilience and Response (EPRR) Policy (OPS 005 V6 March 2019) which* 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.

7.11 **Medicines, Drugs, Prescription Forms and Hazardous Materials**
The Trust will ensure all medicines are strictly controlled. Specific instructions to assist staff in the control and management of medicines are available in its policy document *Medicines Management.* 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.

7.12 **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 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.

7.13 **Lone Working**
The Trust 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 the Trust's policy document: *Lone Worker Policy (HR 042 V4.1 December 2019).*

7.14 **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 considered to be 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 Trust premises by a service user(s) should be removed, stored temporarily in a secure place and the Trust's Security Officer notified immediately. The Security Officer will arrange for 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 Trust 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.

The Trust 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.

8.   **Development, Consultation and Approval**

Name of Policy: Security		**Name of Policy Lead**: Stephen Price	
Date: August 2021		**Contact Details**: (0114) 27 18189	
Consultation Plan:			
Director of Special Projects (Strategy)			
Staff-Side Representatives			
Heads of Service			
General Managers			
Director of Facilities Management			
Executive Director of People			
Chief Pharmacist			
Health and Safety Manager			
Emergency Planning Manager			
Head of Estate Services			
Head of Capital and Strategic Development			
Health and Safety Committee			
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 Special Projects (Strategy)	10 August 2021	No comment received	
Staff-Side Representatives	4 October 2021	Clarification on Section 3 Purpose term 'private accommodation' and responsibility to protect staff	Clarification provided on term 'private accommodation. Policy amended. Section 6 Duties - Heads of Service. Staff protection and Lone Worker Policy
Heads of Service	10 August 2021	No comment received	

		Ref: Purpose: single private dwelling	Policy amended. Section 3 Purpose - private accommodation.
Director of Facilities Management	10 August 2021	Section 6. Duties - EDG	Policy amended. Section 6 Duties - Executive Directors.
		7.12 Counter terrorism - Security Management Director	Policy amended. Section 7 Procedure - 7.12 removed.
Executive Director of People	10 August 2021	No comment received	
General Managers	11 August 2021	No comments	
Chief Pharmacist	10 August 2021	No comment received	
Health and Safety Manager	10 August 2021	No comment received	
Emergency Planning Manager	12 August 2021	Section 6. Duties - Emergency Planning Manager	Policy amended. Section 6 Duties - Accountable Emergency Officer'.
		7.12: Counter terrorism - Security Management Director	Policy amended. Section 7 Procedure - 7.12: removed.
Head of Estate Services	10 August 2021	No comment received	
Head of Capital and Strategic Development	10 August 2021	No comment received	
Health and Safety Committee	10 August 2021	No comment received	

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
Reporting of Incidents	Mechanism of the Risk Management Strategy	Quality and Assurance Committee	Monthly	Quality Assurance Committee	Quality and Assurance Committee	Quality and Assurance Committee

Line 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.

The Security Officer will monitor and review the policy as and when required, every three years or following legislative and NHS requirements.

10. **Implementation Plan**

Action/Task	Responsible Person	Deadline	Progress update
The draft, revised policy submitted to identified individuals and groups for consultation	Security Officer	August 2021	
Final draft sent to the Health and Safety Committee	Security Officer	September 2021	
Health and Safety Committee approve the draft and submit it to the Policy Governance Group	Chair of Health and Safety Committee	September 2021	Draft authorised following approval received from the Chair Staff Side Representatives (5 October 2021)
The Policy Governance Group approve the policy and submit it to the Quality Assurance Committee for ratification	Chair of Policy Governance Group	October 2021	
Policy sent to the Quality Assurance Committee for ratification	Chair of Quality Assurance Committee	October 2021	
Policy placed on the Trust's intranet and internet for dissemination. All previous versions to be removed with an email alert to all staff	Head of Communications	November 2021	
Managers to inform staff for which they have responsibility of the revised Policy	Managers	November 2021	

11.   Dissemination, Storage and Archiving (Control)

Version	Date added to the intranet	Date added to the internet	Date of inclusion in *Connect*	Any other promotion/ dissemination, (include dates)
1.0	July 2005	July 2005	July 2005	
2.0	January 2007	January 2007	January 2007	
3.2	April 2008	April 2008	April 2008	
4.0	October 2010	October 2010	October 2010	
5.0	October 2012	October 2012	October 2012	
6.0	October 2015	October 2015	October 2015	
7.0	December 2018	December 2018	December 2018	
8.0	November 2021	November 2021	November 2021	

Within 5 working days of 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. In addition, Clinical, Service and Support Directors will be instructed to ensure that all teams and areas are made aware of this new/revised policy and how to apply it.

The previous Security Policy, (version 7), will be removed from the Trust intranet and internet 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.*

Line managers are to undertake a staff training needs analysis and consider the type and frequency of training required; this may include:

- SHSC corporate induction.
- Local workplace induction.
- Individual/personal safety awareness based on job description and risk assessment.
- Use and maintenance of security equipment.
- Security protocols/procedures for the workplace, including the rationale behind the protocols.
- Management of situations of potential or actual abuse, aggression or violence, including:
  o understanding the causes
  o recognising the warning signs
  o identifying when and where to get assistance
  o interpersonal skills/defusing techniques

Managers and staff must refer to the Trust's policy *Aggression and Violence: Respectful Response and Reduction* for detailed information.

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

This policy meets various legislative requirements and is necessary to demonstrate compliance with the:

- Health and Safety at Work Act 1974
- Prevention of Crime Act 1953
- Management of Health and Safety at Work Regulations 1999
- SHSC Policy: Health and Safety
- SHSC Policy: Standing Orders, Reservations and Delegation of Powers and Standing Financial Instructions
- SHSC Policy: Scheme of Delegation
- SHSC Policy: Medicines Management
- SHSC's: Risk Management Strategy
- SHSC Policy: Incident Management Policy and Procedure (including Serious Incidents
- SHSC Policy: Aggression and Violence
- SHSC Policy: Emergency Preparedness, Resilience and Recovery (EPRR)
- SHSC Policy: Lone Worker
- SHSC Policy: Fraud, Bribery and Corruption
- SHSC Policy on Policies, which require an Equality Impact Assessment Form, Human Rights Act Assessment Checklist and a Development and Consultation Process: see Supplementary Sections.

14.   **Contact Details**

Title	Name	Phone	Email
Director of Special Projects (Strategy)	Pat Keeling	30 50567	pat.keeling@shsc.nhs.uk
Security and Fire Officer	Stephen Price	27 18189	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 <u>potentially</u> 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, August 2021	**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, August 2021

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?	TBC
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)	N/A
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?	N/A
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?	✔