Healthier Communities, Outstanding Care

Sherwood Forest Hospitals NHS Foundation Trust

TRUST SECURITY POLICY

NON-CLINICAL POLICY

Reference	HS/0006		
Approving Body	Estates Governance Committee		
Date Approved	03/08/23		
For publication to external SFH website	**Positive confirmation received from the approving body that the content does not risk the safety of patients or the public:**		
	YES	**NO**	**N/A**
		*	
Issue Date	August 2023		
Version	8.0		
Summary of Changes from Previous Version	Minor names and committee changes		
Supersedes	7.0		
Document Category	Estates & Facilities		
Consultation Undertaken	Estates Governance		
Date of Completion of Equality Impact Assessment	01/08/2020		
Date of Environmental Impact Assessment (if applicable)	01/08/2020		
Legal and / or Accreditation Implications	N/A		
Target Audience	All members of staff including agency and contract workers		
Review Date	July 2027		
Sponsor (Position)	Associate Director Estates & Facilities		
Author (Position)	Accredited Security Management Specialist		
Lead Division / Directorate	Estates & Facilities - Corporate		
Lead Specialty / Service / Department	Security Management – Estates & Facilities		

Position of Person able to provide Further Guidance/Information	Accredited Security Management Specialist

Associated Documents/ Information	**Date Associated Documents/ Information was reviewed**
1. Lockdown Policy 2. Search Policy 3. 4.	Due 08/2024 Due 02/2024

CONTENTS

APPENDICIES

1.0 INTRODUCTION

This policy document is issued and maintained by the Accredited Security Management Specialist on behalf of the Executive Security Management Director and the Trust, at the issue defined on the front sheet, which supersedes and replaces all previous versions.

2.0 POLICY STATEMENT

Sherwood Forest Hospitals NHS Foundation Trust is committed to providing a safe and secure environment for patients, and for the staff that care for them, and is an essential feature in the delivery of quality health care. Safeguarding the premises and goods from damage or theft helps to ensure that resources can be targeted towards increasing patient services and not diverted to making reparation for acts of crime and vandalism.

There is a basic fundamental need for good practical security measures, which are guided through strong management commitment, undertaken with a sense of responsibility and adequately resource.

Security is concerned with the provision of safeguards against crime and the loss or damage to property and equipment belonging to the Trust, staff, patients and visitors. Security is a management responsibility and involves co-operation from all staff.

Everyone has a duty to behave in an acceptable and appropriate manner. All NHS staff have a right to work, as patients have a right to be treated, free from fear of assault and abuse in an environment that is properly safe and secure.

This policy adheres to all Trust premises and is expected to cover all departements including patient and non-patient areas and apllies to all staff employed by Sherwwod Forest Hospitals NHS Foundation Trust, the students working within the Trust including contractors and volunteers working on behalf of the Trust. The policy is primariliy aimed at protecting the Trsut's employees and resources. The Trust accepts that the NHS has a duty of care towards persons using the servcies and property.

This policy should be read on conjunction with the following:

- Dealing with Violence and Aggression policy
- Incident reporting policy
- Lone worker policy
- Guidance for Police Liaison and Assistance
- Staff Identification Badge & Access Control policy
- Restrictive Practices policy

3.0 DEFINITIONS/ ABBREVIATIONS

Definitions for specific terms used in the policy or procedure.

'The Trust'	means the Sherwood Forest Hospitals Foundation Trust.
'Staff '	means all employees of the Trust including those managed by a third party organisation on behalf of the Trust.
'SMD'	means Security Management Director
'ASMS'	means Accredited Security Management Specialist
'MOU'	means Memorandum of Understanding between ACPO
'NPCC'	means National Police Chief's Council
'DBS'	means Disclosure & Barring Services checks

4.0 ROLES AND RESPONSIBILITIES

The Security Management Director is directly responsible under the directives of the Secretary of State for Health to ensure proper and adequate provisions are in place to protect the safety and security of Patients, visitors and Staff members and to protect the assetts of the Trust from theft or damage.

The Trust Board is responsible for nominating a Non-Executive Director to act as the designated Security Non-Executive Director to work with the Executive Director for monitoring the effectiveness of the security management arrangements in place.

The Security Management Director has appointed a Accredited Security Management Specialist to oversee the requirements to provide a safe and secure environment. The ASMS will develop along with the Trust Executive SMD and the non Executice Director arrangements for a security work plan to deliver, review and develop the security of assets, property and people.

The role of the ASMS is set out by the NHS Standard Contract. Support is provided by the Trust ASMS and SMD. The role specifically includes the provision of professional skills and expertise in four main strands of security management work.

- Tackling violence against staff and professionals working in the NHS
- Ensuring the security of property and assets
- Ensuring the security of drugs, prescription forms and hazardous materials
- Ensuring the security of paediatric and maternity wards and areas

Divisional and departmental managers have a responsibility for the protection and security of physical assets and equipment that belong to the Trust. It is essential that proper measures be in place for the auditing of all assets.

All those who work in, use or provide services to the NHS have a collective responsibility to ensure that property and assets relevant to the delivery of NHS healthcare are properly secure.

5.0 APPROVAL

Estates Governance Committee

6.0 DOCUMENT REQUIREMENTS

6.1 Security

Sherwood Forest Hospitals NHS Foundation Trust maintains a separate policy that tackles violence and aggression for the protection of their staff and ensuring that the healthcare environment is safe and secure. Local procedures recognise that taking action is appropriate where physical assault and/or non-physical assault is likely to:

- Prejudice the safety of staff involved in providing care or treatment; or lead the member of staff providing care to believe that he/she is no longer able to undertake his/her duties as a result of fearing for their safety
- Prejudice any benefit the patient might receive from the care or treatment
- Prejudice the safety of other patients; or
- Result in damage to property inflicted by the patient, relative, visitor or as a result of containing them.

6.2 Sherwood Forest Hospitals NHS Foundation Trust maintains a close working relationship with the wider community through the Mansfield and Ashfield Community 'RESPECT' Partnership Forum. The Trust ASMS is a member of the Tasking and Co-ordination group and liaises with the anti-social behaviour team and local management beat officers of Nottinghamshire Police. A local Memorandum of Understanding is in operation and signed off by the respective Nottinghamshire Police representative and the Chief Executive of Sherwood Forest Hospitals NHS Foundation Trust.

6.3 When initiating sanctions, a range of measures will be considered by the Trust depending on the severity of any inappropriate actions. This may assist in the management of unacceptable behaviour by seeking to reduce the risks and demonstrate acceptable standards of behaviour. These may include:

- Making staff aware of the process and the support available to them when an incident takes place
- Educating staff on the importance of reporting procedures because it will ensure all incidents are recorded and appropriate measures are taken
- Post incident support and counselling to support staff in order that they may return to work which will encourage staff to remain working within the healthcare environments in the long term
- The creation or development of the existing pro-security culture
- Training
- Verbal warnings
- Written warnings
- Civil injunctions and nationwide Anti-Social Behaviour Orders (Asbo's)
- Criminal prosecution

6.4 In order to comply with the NHS Standard Contract the Trust has identified seven generic areas of action for both proactive and reactive initiatives in relation to security management. This process is included as the basis for the delivery of a safe and secure environment throughout Sherwood Forest Hospitals NHS Foundation Trust:

- Engendering a **Pro-security culture**
- **Deterring** security incidents and breaches
- **Preventing** security incidents and breaches
- **Detecting** security incidents and breaches where they have not been prevented.
- **Investigating** security incidents and breaches in a professional, objective, and fair manner where detected, and ensuring that lessons are learnt and system weaknesses are fed into risk assessments, policy development and revision to prevent further breaches from occurring.
- Applying a wide range of **Sanctions** where necessary and appropriate
- Seeking **Redress** to ensure that funds are put back into the NHS for improved clinical care.

6.5 **Pro-Security Culture**

The development of a pro-security culture is integral to all strands of security management work in the NHS. Building a pro-security culture is about taking an inclusive approach with all those involved – staff, managers, patients / service users and the public.

The Trust Accredited Security Management Specialist will lead on work in developing a pro-security culture; collective responsibility, partnership working and local ownership are essential to achieving the implementation of robust procedures and systems. Managers should communicate to staff what they can expect in terms of support and what is expected from them. Local procedures reflect:

- The views of staff and their union safety representatives or professional representatives
- The views of patients, service users and their representatives
- Clear links to other relevant procedures and existing health body policies
- Clear outline of responsibilities and lines of accountability in respect of any action to tackle all untoward incidents or breaches in security.
- Legal advice from the NHS health body's' own legal team on the precise terms and application of procedures in appropriate cases

It is essential that staff, at all levels, are made aware of their responsibility to be familiar and compliant with procedures that are in place for their protection. This is facilitated through using:

- Job Descriptions
- Clearly written procedures
- Induction Programmes
- Presentations by ASMS
- Awareness-raising sessions by risk managers
- Training

- Team Briefings
- Health body
- Intranet

6.6 **Deterrence**

Using publicity and the media, both nationally and locally, is a highly effective method of promoting what the Trust and the NHS are doing to better protect those who work in healthcare environments and protect the property of the Trust.

The ASMS and the Trust Communications Department have established good relationships with the press and the media to ensure the appropriate level of publicity is in place for measures introduced by the Trust and the NHS to better protect staff and the Trust. A true deterrent effect can only be achieved when:

- There is some certainty that potential offenders will be apprehended.
- They understand that they will be punished for their actions; and
- The sanctions that may be applied against them outweigh any perceived benefit they may derive from their actions.

In addition, to play a key role in helping to protect the Trust, its staff and patients, appropriate publicity of cases involving sanctions applied to those who have offended, may also serve to deter others who may be mindful to commit such acts.

6.7 **Prevention**

Prevention should be based on effective use of available information to ensure that the risk of future incidents can be minimised - this includes learning from operational experience on previous incidents and adopting an inclusive approach that involves staff.

The key to preventative action is an honest and objective appraisal and understanding of how and why incidents can occur in healthcare environments and learning from this. In order to achieve this, the following factors should be considered:

- Type of incident (for example, non-physical/physical assault, theft, criminal damage)
- Severity of incident
- Cost to NHS health body (human and financial)
- Individuals and staff groups involved.
- Weaknesses or failures that have allowed these incidents to take place, for example, procedural, systems or technological.
- Training needs analysis of staff, in relation to the prevention and management of violence, crime prevention, operational response etc.
- Review of measures in place to manage risk.
- Appropriate use and operation of technology such as CCTV

General Considerations for Assessing Risk

Prevention is about using information to ensure that risk of similar future incidents occurring can be minimised. Sherwood Forest Hospitals NHS Trust strives to ensure that they have adequate arrangements in place to assess risk to their staff, patients, and property. This information is needed to make decisions on how to manage those risks so that the decisions are made in an informed, rational and structured manner and that the action taken is proportionate. Arrangements also need to be put in place to monitor and review the findings. Robust risk assessments are being carried out locally, contributing factors assessed or post-incident reviews performed as appropriate. Risk assessments will link into the risk management strategy and will be included on the Trust risk register.

Exercise Positive Reporting Practices

Staff are actively encouraged to report all incidents relating to security related incidents or suspicious occurrences – the information in the first instance need only be concise relating to the incident in question. This will help to provide a clearer picture with regard to the extent of the problems.

Physical Security Measures

There are a range of physical security measures in operation that add further value alongside consistent and thorough policies and procedures.

Robust risk assessments carried out locally, contributing factors, post-incident reviews and analysis of reports and operational information may highlight the need to introduce technology to minimise risk the risk of violence and aggression.

Design of areas and departments are consistently considered as part of any changes that make the environment more comfortable, aesthetically pleasing, and reduce the possibility of creating a crime target. Design characteristics such as distance between beds/treatment areas, reduced noise, improved lighting, better ventilation, better ergonomic designs, and supportive workplaces are some of the features, which help reduce the potential to commit crime or disorder. These design factors are considered when planning any new builds or refurbishment of existing healthcare premises.

Technology plays an important part in ensuring physical measures are adequately implemented. Robust risk assessments are carried out locally, contributing factors, post-incident reviews and analysis of reports and operational information may highlight the need to introduce technology to minimise the risk within the healthcare environment.

Consideration is given to the most used technology measures, including the use of:

- CCTV surveillance equipment
- Access control
- Intruder alarm systems
- Personal alarms and protection equipment
- Asset tagging and security marking.
- Improved and enhanced lighting levels
- Physical locks

- Window restrictors

Individual Locking Systems are provided as follows:

- To all external doors
- To department access doors into those departments that are not staffed on a 24 hour basis
- To certain doors within departments, giving access to higher security areas.
- To cupboards, cabinets etc., the contents of which are valuable or potentially hazardous.

High-risk and vulnerable areas that are not staffed on a 24hour basis are also provided with automatic intruder alarms and, where practicable, relayed to the central control point at the hospital telecommunications and help desk facility. From there, a pre-determined plan of action is instigated to ensure a quick response by the Police and the on-site contracted security services.

The Trust Medical Equipment Management Department mark all medical devices which serve as an element of security marking. The Health Informatics also consistently marks high value items of IT equipment.

It is recognised that where technology systems are in operation, back-up procedures need to be in place to ensure safety and security of staff and premises is provided should there be a temporary loss of operation.

The secure lock down policy for the trust premises is to be used and utilised alongside in addition to the Trust security policy.

Guarding Services

The security guarding services are contracted to provide a 24-hour security services throughout the Trust premises. The security management company and its operatives are required to hold and maintain registration with the Security Industry Authority, including the need to have CRB checks.

The security guarding services provide and are responsible for but not limited to:

- Security patrols
- Static guarding post during evening periods
- Physical check of premises to ensure the security of areas.
- Protection of property and assets
- Escort of staff in and around the site
- The observation of suspicious persons and the removal of offenders from the trust premises
- Response to monitoring equipment actuations-intruder alarms, panic alarms etc
- The monitoring of the site and all activities using the Trust CCTV systems, panic alarms or other devices installed for the safety and protection of staff, the public and property.

- Supporting staff during incidents including violence and aggression
- Liaison with the Trust management and site co-ordinators
- Liaison with the Police
- Assist the trust with the lockdown procedures for vulnerable areas or during emergency incidents including major incidents.

CCTV Operational Network

Sherwood Forest Hospitals maintain a system of networked CCTV, which are monitored by the security guarding services contractor at a central control room. The equipment and operations are reviewed by the Trust ASMS, via the network system who has the responsibility for providing any footage or reviewing requested by the Police or other lawful authority for evidential purposes.

The CCTV equipment records images onto a hard drive through the integrated installation. The hard drive has the capacity to retain images for a period no less than 14 days surveillance.

The images remain the property of the Trust under information governance guidance and procedures. Any concerns over the release of data should be referred to the trust Information Governance lead officer.

Responsibility for security of CCTV systems recorded information is held by the contracted security service provider. Access to CCTV footage is only available or permissible by contacting the Trust ASMS or out of hours via the on-call silver command in the first instance. This is to ensure that information which may have the potential use for legal evidence remains secure and confidential.

The Trust uses various means to try and reduce incidents including:

- Designing out risks when areas are constructed or redeveloped. The Trust will work towards the Secure by Design Hospitals Guidance which seeks to create a safe and secure working environment for patients, medical professionals, and visitors. The provision of a safe environment should significantly reduce the opportunity for crime. Secure by Design is endorsed by the National Police Chief's Council (NPCC) and has the backing of the Home Office Crime Reduction Unit.
- Use of access control systems to prevent and restrict unauthorised access and provide security to areas.
- Installation of intruder alarm systems to detect intrusion into areas or attempts to gain unauthorised access.
- Use of panic alarm systems for areas identified under risk assessment as high risk of unacceptable or potential for violent behaviour which requires an early intervention and response by the security guarding services.
- Use of CCTV systems for evidential purposes to assist in the prosecution of individuals committing offences on Trust premises or offences against staff.

6.8 **Detection**

Detection or incident reporting is an integral part of the security management process. It allows the necessary information to be gathered to:

- Identify the problem.
- Assess and manage the risk.
- Develop solutions.

Incident reporting is the key to the detection of all acts of crime and disorder. Detection allows appropriate incidents to be investigated by the Trust ASMS to ensure that lessons learnt can be fed back into management procedures. It also facilitates the development or revision of policy, procedures, or systems to ensure that the risk of similar incidents occurring again can be minimised.

All staff should be made aware of what, how, when and to whom any security related incident should be reported.

Reporting of incidents will ensure that any lessons learnt can be fed back into risk management processes and further preventive measures can be developed, and sanctions applied (where appropriate). In turn, these examples can be used to increase publicity to enhance the deterrent effect.

This will also assist in the review of procedures ensuring that they are developed and revised to minimise the risk of, and the potential for, similar incidents reoccurring.

In short, this fosters a pro-security culture amongst all staff and professionals, raising their awareness of how and why incidents should be reported, how it facilitates the prevention process and help to ensure their further security and safety.

6.9 Incident Reporting and Investigation

All incidents or near misses, no matter how small, must be reported through the trust Datix incident reporting system, policy, and procedures. The incident reporting policy is to provide the staff of the trust with a working procedure for dealing with adverse incidents and to improve patient, staff, visitor and contractor safety and the protection of trust assets and personal items.

All incidents must be reviewed by the line manager and where it is deemed appropriate in terms of a security related incident, the risk must be reported to the ASMS.

Following an incident that has occurred, or suspected as having occurred the ASMS must ensure that effective arrangements have been put in place to determine that incidents, including potential risks, are reported, and dealt with in accordance with frameworks for tackling security management work.

In all incidents, irrespective of whether they or the police may be pursuing sanctions against offenders, ASMS should investigate to establish the causes of the incident and whether any further action needs to be taken in the areas of pro-security culture, deterrence, prevention or detection.

It is essential that where lessons can be learnt that they are fed into revisions of procedures and systems locally, as well as guidance nationally, to ensure that staff are provided with the best possible protection, if the risks they face are to be minimised. The structure of ASMS and SMD

locally across the NHS, with partnership working with other local Trusts ASMS's, will ensure that there is an effective mechanism in place to facilitate this process.

Regulation of Investigatory Powers Act 2000 (RIPA)

Before any type of surveillance is undertaken it must be discussed with the Security Management Director in conjunction with the Trust ASMS. An assessment as to whether the surveillance comes under the requirements of RIPA will be completed. If it is considered necessary, an application will be undertaken for Nottinghamshire Police to perform the surveillance operation in the first instance.

No covert surveillance can be carried out unless it is sanctioned and authorised by the police.

Covert surveillance is defined as surveillance carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is taking place.

6.10 **Sanctions**

There is a range of sanctions, which the Trust will consider to be taken against individuals (or groups) who abuse NHS staff and professionals, or who steal or inflict damage on its property. These range from criminal prosecutions, Anti-Social Behaviour Orders (ASBO) through to civil injunctions.

Action and range of sanctions that will be considered when an assault, public disorder offence or other crime takes place includes:

- Verbal warning
- Written warning.
- Acknowledgement of Responsibility Agreement or Pre-Treatment Agreement is an intervention designed to engage an individual in acknowledging his or her anti-social behaviour and its effect on others, with the aim of stopping that behaviour.
- Local sanctions such as managed visits where a known violent patient may be escorted at all times by Security when on health body premises or police involvement.
- Injunctions
- Nationwide Asbo's
- Criminal & Civil sanctions
- Bail conditions

Sanctions are considered to be an effective way of deterring individuals from committing an offence. The type of sanctions applied should be adequate to the severity of the offence, in other words the list of sanctions mentioned above do not have to be considered in an progressive manner. For example, if a patient has physically injured a member of staff causing broken ribs, and skin and severe bruising, the Trust can straight away consider criminal and civil sanctions.

6.11 **Redress**

Incidents - whether they involve assaults on staff, theft of, or damage to Trust property have a direct impact on both the human and financial resources allocated to the Trust, needed to

deliver high quality patient care. Through good investigative work by the ASMS, the Trust will be able to identify resources lost as a direct result of an incident, providing the necessary information and evidence to attempt to recover that loss, whether through the criminal courts, by way of compensation, or seeking redress through the civil courts.

Two principles lie behind effective recovery:

- Monies lost through violent incidents against Trust staff, theft of, or damage to, Trust property can be returned to patient care; and
- Recovery of losses delivers an important deterrent message to staff, patient/service users and the public, that crime simply does not pay, and that the Trust will always pursue redress from those who attack it and deprive it of valuable resources.

6.12 **Risk Assessment and Audit**

As part of the process for investigation of an incident, it is important that a risk assessment should be carried out by the investigator. This for some incidents may only need to be as included within the IR2 investigation tool of the incident reporting system.

If the incident is such that it has the potential to present an on-going security risk to the physical security of the premises or any asset held by the department, the incident must be raised by the department or local manager for corrective action if able or highlighted within the divisional governance process and if considered as an on-going risk, entered on the divisional risk register for further consideration and action.

Where the incident is deemed to be substantial, the associated risk may require adding to the trust risk register and brought to the attention of the trust risk management group for consideration and action.

The department lead with have the responsibility to ensure the risk is added to the register where considered appropriate. The risk remains the responsibility of the Divisional General Manger unless advised otherwise by the risk management committee.

The ASMS will conduct a crime reduction or security survey of all security risks brought to their attention. A written report will be provided for the attention of the appropriate line manager or management team for advice and action.

The ASMS will also conduct a rolling programme of site wide security audits to provide assurance that the security strategy for the operations of the buildings is effective.

The ASMS will report and update the trust Estates Governance committee of any significant risks and will provide the trust with an annual security report which will include an overview of security risks.

The Flowchart summarises the Risk Assessment Process

IDENTIFY THE RISK/THREAT/DANGER
That is anything with the potential to cause harm or risk.
Incident raised by the department or local manager.

↓

DECIDE WHO MIGHT BE HARMED

There is no need to list individuals by name but consider the groups of people and numbers etc.

Risk assessed by the department or local manager.

↓

WHAT EXISTING CONTROLS MEASURES DO YOU HAVE IN PLACE

This means looking at the preventative and protective measures already taken.

Action plan prepared by the department manager

↓

EVALULATE THE RISK IS MORE NEEDED TO CONTROL THE RISK

For the Hazards listed in your risk assessment do the precautions already taken:

- Meet the standards set by legal requirements.
- Comply with recognised industry standard.
- Represent good practice.
- Minimise the risk to the lowest level possible

  Have you provided?
- Adequate information, instruction, and training to those who need to know.
- Are adequate systems or procedures in place?
- Where the risk assessment is not adequately control indicate what more you need to do in the Observations and recommendations to improve safety column of the risk assessment

Consider a full risk assessment by the trust ASMS.

↓

REVIEW AND REVISE

The risk assessment should be reviewed or reassessed at least annually, where there are any changes, or where an incident or near miss has occurred.

Review undertaken by the department or local manager.

7.0 MONITORING COMPLIANCE AND EFFECTIVENESS

Minimum Requirement to be Monitored (WHAT – element of compliance or effectiveness within the document will be monitored)	Responsible Individual (WHO – is going to monitor this element)	Process for Monitoring e.g. Audit (HOW – will this element be monitored (method used))	Frequency of Monitoring (WHEN – will this element be monitored (frequency/ how often))	Responsible Individual or Committee/ Group for Review of Results (WHERE – Which individual/ committee or group will this be reported to, in what format (eg verbal, formal report etc) and by who)
Effectiveness of the procedure	Author, Ward / Service, Department Managers,	Review in line with National / Local Guidelines / Guidance	Formal review on a 3-year basis in line with Trust Risk Assessment	Accredited Security Management Specialist, Estates Governance Committee
Monitoring incidents and learning	Accredited Security Management Specialist, Department Managers,	Review in line with the procedure	Activity within the incident feedback / de-brief procedure	Accredited Security Management Specialist, Estates Governance Committee

8.0 TRAINING AND IMPLEMENTATION

The Trust's Incident reporting procedure will be used to monitor the effectiveness of this policy.

The annual security report submitted to the Estates Governance Committee will include data on the level of incidents reported.

The Estates Governance Committee will consider a range of measures relating to incidents and breaches in security. These will include reports on the number of reported incidents.

Divisional performance management reports include information on statistics and activity on a quarterly basis.

The Trust will be audited under the NHS Standard Contract for performance management under the security standards and monitored through the annual submission of the security annual report, ASMS work plan and other related tasks/topics.

Training needs analysis dictates what other training might be required in the future and a key part of the healthcare delivery service is the ability to communicate effectively and provide good customer service. Training is provided as part of the induction process for new staff as well as on an on-going basis to update and educate existing staff.

9.0 IMPACT ASSESSMENTS

Equality Impact Assessment

The Trust is committed to ensure that none of its policies, procedures and guidelines discriminate against individuals directly or indirectly on the basis of gender, colour, race, nationality, ethnic or national origins, age, sexual orientation, marital status, disability, religion, beliefs, political affiliation, trade union membership, and social and employment status. An EIA of this policy/guideline has been conducted by the author using the EIA tool developed by the Diversity and Inclusivity Committee. (28-12-2016)

Environmental Impact Assessment

An Environmental impact assessment has been undertaken on this policy and has not indicated that any additional considerations are necessary.

10.0 EVIDENCE BASE (Relevant Legislation / National Guidance) AND RELATED SFHFT DOCUMENTS

Evidence Base:

Secretary of State Directions to health bodies on dealing with violence against NHS staff (2003) and security management measures (2004).

Related SFHFT Documents:

- Lock down policy.
- Violence & Aggression policy
- Restrictive Practices policy
- Search policy
- CCTV policy
- Major incident policy
- Terrorism and Bomb threat guidance
- Missing persons policy

11.0 KEYWORDS

12.0 APPENDICES

- Equality Impact Assessment (EQUI) Form
- Environmental Impact Assessment
- Policy and Implementation Plan (Template)
- Clarification of Employee awareness

APPENDIX 1 - EQUALITY IMPACT ASSESSMENT FORM (EQIA)

Name of service/policy/procedure being reviewed:			
New or existing service/policy/procedure:			
Date of Assessment:			
For the service/policy/procedure and its implementation answer the questions a – c below against each characteristic (if relevant consider breaking the policy or implementation down into areas)			
Protected Characteristic	**a) Using data and supporting information, what issues, needs or barriers could the protected characteristic groups' experience? For example, are there any known health inequality or access issues to consider?**	**b) What is already in place in the policy or its implementation to address any inequalities or barriers to access including under representation at clinics, screening?**	**c) Please state any barriers that still need to be addressed and any proposed actions to eliminate inequality**
The area of policy or its implementation being assessed:			
Race and Ethnicity	Availability of this policy in languages other than English	Alternative versions can be created on request	None
Gender	None	Not Applicable	None
Age	None	Not Applicable	None
Religion	None	Not Applicable	None
Disability	Visual accessibility of this document	Can be created in font size 14. Use of technology by end user. Alternative versions can be created on request	None
Sexuality	None	Not Applicable	None
Pregnancy and Maternity	None	Not Applicable	None
Gender Reassignment	None	Not Applicable	None
Marriage and Civil Partnership	None	Not Applicable	None

Socio-Economic Factors (i.e. living in a poorer neighbourhood / social deprivation)	None	Not Applicable	None

What consultation with protected characteristic groups including patient groups have you carried out?

- None for this version

What data or information did you use in support of this EqIA?

- Trust policy approach to availability of alternative versions

As far as you are aware are there any Human Rights issues be taken into account such as arising from surveys, questionnaires, comments, concerns, complaints or compliments?

- No

Level of impact

From the information provided above and following EQIA guidance document Guidance on how to complete an EIA (click here), please indicate the perceived level of impact:

Low Level of Impact

For high or medium levels of impact, please forward a copy of this form to the HR Secretaries for inclusion at the next Diversity and Inclusivity meeting.

Name of Responsible Person undertaking this assessment:
Wesley Burton

Signature:

Date:
August 2020

APPENDIX 2 – ENVIRONMENTAL IMPACT ASSESSMENT

Use this appendix if it is applicable by completing all rows of the last two columns or delete

The purpose of an environmental impact assessment is to identify the environmental impact, assess the significance of the consequences and, if required, reduce and mitigate the effect by either, a) amend the policy b) implement mitigating actions.

Area of impact	Environmental Risk/Impacts to consider	Yes/No	Action Taken (where necessary)
Waste and materials	• Is the policy encouraging using more materials/supplies? • Is the policy likely to increase the waste produced? • Does the policy fail to utilise opportunities for introduction/replacement of materials that can be recycled?	No No No	Not Applicable
Soil/Land	• Is the policy likely to promote the use of substances dangerous to the land if released? (e.g. lubricants, liquid chemicals) • Does the policy fail to consider the need to provide adequate containment for these substances? (For example, bunded containers, etc.)	No No	Not Applicable
Water	• Is the policy likely to result in an increase of water usage? (Estimate quantities) • Is the policy likely to result in water being polluted? (e.g. dangerous chemicals being introduced in the water) • Does the policy fail to include a mitigating procedure? (e.g. modify procedure to prevent water from being polluted; polluted water containment for adequate disposal)	No No No	Not Applicable
Air	• Is the policy likely to result in the introduction of procedures and equipment with resulting emissions to air? (For example, use of a furnaces; combustion of fuels, emission or particles to the atmosphere, etc.) • Does the policy fail to include a procedure to mitigate the effects? • Does the policy fail to require compliance with the limits of emission imposed by the relevant regulations?	No No No	Not Applicable
Energy	• Does the policy result in an increase in energy consumption levels in the Trust? (Estimate quantities)	No	Not Applicable
Nuisances	• Would the policy result in the creation of nuisances such as noise or odour (for staff, patients, visitors, neighbours and other relevant stakeholders)?	No	Not Applicable

APPENDIX 3

POLICY / PROCEDURE IMPLEMENTATION PLAN

(TEMPLATE)

Document Reference	HS / 0006
Title	Trust Security Policy
Version	8.0
Date	July 2023
Lead officer for implementation	Accredited Security Management Specialist
Target Audience	All Staff
Training and Education Requirements	All staff will go through their mandatory training to keep them up to date on current issues and processes. All new starters will receive this training on orientation.
Implementation Plan	Divisional and departmental managers are responsible for ensuring staff have appropriate training to ensure compliance with this policy. Awareness of this policy will be integrated through mandatory training and new staff orientation day.
Timetable for Completion of Implementation	On going

Note 1: Where any formal training and education requirement is identified, the policy should include reference to whether it is:

- Statutory - mandated by law
- Mandatory - mandated by external policy or standards or by SFHFT
- Essential - imperative for delivery of our strategic objectives

A common alternative to formal training and education may be a requirement to inform / communicate with employees (which does not necessitate training however can often be mistaken as training). An appropriate method of communication should be put in place - however it is not a training need.

If training and education is required, the target staff groups should be clearly identified as should any need (and frequency) for refresher training.

If training and education is a required part of the policy, authors should identify the following systems:

- How the training topic will be incorporated in the trust's training needs analysis (TNA)
- Resources for design and delivery of training
- How the target audience will access the training
- Recording and reporting of attendance
- How attendance will be monitored and managed
- The timetable for completion of policy implementation

APPENDIX 4

CERTIFICATION OF EMPLOYEE AWARENESS

Document Title	Trust Security Policy
Version (number)	8.0
Version (date)	July 2023

I hereby certify that I have:

- Identified (by reference to the document control sheet of the above policy/ procedure) the staff groups within my area of responsibility to whom this policy / procedure applies.
- Made arrangements to ensure that such members of staff have the opportunity to be aware of the existence of this document and have the means to access, read and understand it.

Signature	
Print name	
Date	
Division / Directorate	

The manager completing this certification should retain it for audit and/or other purposes for a period of six years (even if subsequent versions of the document are implemented). The suggested level of certification is;

- Clinical Divisions – Divisional General Manager or nominated deputies.
- Corporate Directorates - Deputy Director or equivalent.

The manager may, at their discretion, also require that subordinate levels of their directorate / department utilise this form in a similar way, but this would always be an additional (not replacement) action.