|  |  |
| --- | --- |
| **Document name:** | Security Management Policy |
| **Document type:** | Policy |
| **What does this policy replace?** | Policy review |
| **Staff group to whom it applies:** | All staff within the Trust |
| **Distribution:** | The whole of the Trust |
| **How to access:** | Intranet and website |
| **Issue date:** | February 2022 |
| **Next review:** | February 2025 |
| **Approved by:** | Executive Management Team |
| **Developed by:** | Trust Security advisor |
| **Director leads:** | Associate Director of Estates and Facilities |
| **Contact for advice:** | Security advisers:   * 07771345275 * 07920535209   Head of Safety, Security and Risk:   * 07967378867 |

**CONTENTS**

**Page**

**Quick Reference Guide**

**1. Introduction 1**

1.2 Overarching Security Statement **3**

1.3 Core Security Principals **3**

**2 Purpose 4**

2.1 Security Management Strategy  **5**

**3 Scope 6**

**4 Definitions 6**

**5 Duties and Responsibilities 6**

5.1 The Chief Executive **6**

5.2 South West Yorkshire Partnership NHS Trust Board **6**

5.3 Associate Director of Estates and Facilities (SMD) **7**

5.4 Directors 7

5.6 Head of Safety, Security and Risk **8**

5.7 Security Advisors **9**

5.8 Local Counter Fraud Specialist 9

5.9 Human Resources Managers **9**

5.10 Reducing Restrictive Physical Interventions Team Leader **9**

5.11 Health & Safety Advisors **9**

5.12 Security Officers **9**

5.13 Contracted Security Service Provider **10**

5.14 All Managers and Staff **10**

**6. Process 10**

**7. Training Requirements 11**

**8. Sanctions 12**

8.1 Criminal **12**

8.2 Civil Courts **13**

8.3 Civil Action  **13**

8.4 Injunctions  **14**

8.5 Claims for Compensation/Damages **14**

8.6 Personal Injury **14**

8.7 Hate Crime **14**

8.8 Anti-social behaviour **14**

8.9 CBOs (Criminal Behaviour Orders) CPIs (Crime Prevention injunction) **15**

**9 Redress 15**

9.1 Recovery

9.2 Decision on redress

9.3 Communications of prosecution

**10 Development process 17**

**11 Approval and ratification 18**

**12. Process for Review 18**

**13. References 18**

**14. Dissemination 19**

**15. Implementation 19**

**16. Monitoring for compliance 19**

**Appendix A: Version Control 21**

**Appendix B: Equality Impact Assessment 22**

**Appendix C: Checklist for review and approval for procedural documents 25**

**1. Introduction**

In accordance with NHS Standard Contract, South West Yorkshire Partnership NHS Foundation Trust (SWYPFT) has appointed 2 Security Advisers, who are also historic accredited Local Security Management Specialists. The Security Advisor operates within the clear legal framework set by NHS England, with clearly defined duties and responsibilities.

Apart from the contractual requirements, SWYFPT is subject to assessment by the Care Quality Commission (CQC). They have recognised the importance of security in their assessment process, with specific security references in Fundamental Standards (Premises and Equipment – Regulations 15).

The Trust also employs other Specialist Advisors to advise on the matters of Management of Security, Reducing Restrictive Physical Interventions, Health and Safety and Emergency Planning.

Security risks can be expensive in terms of resources, time, finance and convenience; therefore it is essential that security management is effective, efficient and commensurate with the threat.

The threat is defined as the illegal and unacceptable activities that seek to disrupt or cause distress to people and property.

* 1. **Overarching Security Statement**

Protective security, including physical and personnel security, is an essential enabler to ensuring the trust works more efficiently. Security risks must be managed effectively, collectively and proportionately, to achieve a safe and secure environment for the provision of high quality healthcare to the local community.

**1.2 Core Security Principals**

Ultimate responsibility for security lies with the Chief Executive and the Board. Business Development Units and Services, via Directors, must manage their security risks within the parameters set out in this framework and as laid out within the security related policies as ratified by the Board.

All managers and employees (including contractors and volunteers) have a collective responsibility to ensure that NHS assets (information, personnel and physical) are protected in a proportionate manner from all illegal or malicious activity.

Directorates and services must be able to share information (including personal data) confidently knowing it is reliable, accessible and protected to NHS Information Governance standards irrespective of format or transmission mechanism.

The procedures described here are compliant with the strategy provided by NHS Protect (now disbanded). This procedure is extended to include protection to all patients/service users, visitors and to the wide variety of staff working across the organisation.

**2. Purpose**

The aim of this Policy is to develop and implement the trust security strategy to protect staff and trust assets, so that it can provide high quality healthcare to the public and take all practicable steps to protect the property of our patients while they are admitted to our care.

Physical, technical and procedural controls need to be balanced to achieve an appropriate security approach that meets the needs and circumstances of any service/locality.

It is important that the Trust protects its assets and people from exposure to the effects of crime, in particular violence and harassment, if all staff are to feel secure and able to treat patients effectively. Similarly patients need to feel secure in the environment in which they are treated.

The fundamental principles of security within the Trust will be:-

* To develop a high level of security awareness among staff and patients and encourage them to report security related incidents so that consideration can be given to taking further action against the perpetrators where identified.
* Where appropriate, use internal and external communications to raise awareness of those who have or for those who are minded to be dishonest or violent towards Trust staff, patients and property/assets; both of the consequences of their actions to themselves and others, to assist in deterrence of further incidents.
* To deny the opportunity for crime and to deter criminal activity, as far as possible.
* To detect crime when it is committed and by working with the Police, Crown Prosecution Service and NHS Protect to ensure a national approach to the investigation of security incidents.
* To respond effectively to incidents and security related events.
* To record, report and analyse security-related incidents/trends in order to seek improvements and reduce risk.
* To raise the profile of personal safety and security across the Trust in order to build staff confidence and encourage individual responsibility.
* To promote the Trust’s position regarding the unacceptability of violence and aggression against staff.
* To ensure the full range of possible sanctions is considered when dealing with offenders and to obtain redress in appropriate cases.

**2.1 Strategy**

The Security Management Strategy will ensure that a clear business process model will be applied in respect of security management.

The key elements are:

* Identifying problems by analysis of risks and trends.
* Working within a clear strategic framework which establishes a common language of aims, objectives and methodologies.
* Creating a strong and flexible working structure which can focus collective, professional expertise on the issues to be addressed.
* Using the structure to carry out a range of actions in respect of each specific area where security needs to be strengthened.
* Engage fully with the SMD in regard to ensuring work undertaken meets common, high national standards; and continuously review policy and procedure to learn from operational experience to minimise risks and prevent future security related incidents from occurring.

At the core of the strategy is the recognition that all security management work must be based on clear and unambiguous risk identification and assessments.

Areas identified as needing specific policy and direction include:

* Management of violence and aggression against staff
* Lone worker safety
* Physical security of sites, buildings, wards and departments including Lockdown arrangements
* Personnel Security
* Protection of NHS assets
* Protection of patient property
* Security related major incidents
* Electronic security systems (CCTV, Intruder Alarms and Access Control Systems etc.).
* Where appropriate, applying a range of sanctions against those who commit crime.

**3. Scope**

This strategy applies equally to all executives, managers, directly and indirectly employed staff, contractors and volunteers working on behalf of SWYPFT.

**4. Definitions and Abbreviations**

* Access Control – managing access to/from and around a defined protected area to prevent unauthorised persons from gaining access. Can be achieved by electronic, mechanical or operational (guard/receptionist) means
* CCTV – Closed Circuit Television
* Information Governance/Security is the protection of all information whether held electronically or in physical formats
* Sanctions - A provision of a law enacting a penalty for disobedience
* Redress - The setting right of what is wrong
* LSMS – Local Security Management Specialist, (accredited trained person) NHS

* SMD – Security Management Director
* Security: the protection of people, information, material activities, reputation and facilities against harm, loss or unauthorised disclosure
* CQC – Care Quality Commission, CCG – Clinical Commissioning Group
* LCFS – Local Counter Fraud Specialist

**5. Duties and Responsibilities**

**5.1 The Chief Executive**

The Chief Executive is responsible for ensuring that SWYPFT complies with current security directions and legislation and is ultimately accountable for all matters of security. The Chief Executive has the overall responsibility and accountability for security to ensure that minimum standards of good practice are developed whilst SWYPFT Policies and Procedures are developed, and subsequently embedded within the organisation.

**5.2 Trust Board**

SWYPFT Board is responsible for ensuring that legal obligations are met in line with the risk management agenda and that resources are made available to ensure that the premises are maintained in a physically secure condition.

**5.3** **Associate Director of Estates and Facilities / Security Management Director (SMD)**

|  |  |  |
| --- | --- | --- |
| It is the responsibility of the Associate Director of Estates and Facilities, so far as reasonably practicable to: | | |
| * Act as the Security Management Director (SMD) for the Trust. | | | |
| * Co-ordinate all security management matters across SWYPFT. | | | |
| * Ensure a fit for purpose Security Management Policy that reflects all of the safety strategy of SWYPFT is in place. | | | |
| * Ensure financial resources are available, in conjunction with the Director of Finance and colleagues in order to implement relevant security management arrangements. | | | |
| * Ensure appropriate arrangements are in place to periodically monitor the security management performance of the organisation. * Report to the Trust Board on an annual basis the security management performance of SWYPFT. * Bring to the attention of the Associate Director of Estates and Facilities any matter that has a bearing on the Security Management arrangements of the Trust. * Ensure staff within their control attends appropriate training as required by risk assessment, policy, statutory directive, appraisal or agreement. * Offer direct line management support and guidance to Head of Safety, Security and Risk and Security Advisors. | | | |
| **5.4 Directors** | |
| It is the responsibility of Directors, so far as reasonably practicable to: | |
|  | Be responsible for all aspects of health, safety and welfare of employees under their management, including Security Management Arrangements. |
|  | Be responsible for the health, safety, security and welfare of any person who could be affected by activities over which the Director has management responsibility. |
|  |  |
|  | Ensure strategic BDU security related assessments are undertaken, monitored, practiced and managed within their areas of responsibility. |
|  | |
|  | |
|  |  |

**5.5 Head of Safety, Security and Risk**

It is the responsibility of the Head of Safety, Security and Risk, as far as reasonably practicable to

|  |
| --- |
| * Offer direct line management support and guidance to SWYPFT Security Advisors. * Bring to the attention of the Associate Director of Estates and Facilities any matter that has a bearing on the Security Management arrangements of the Trust. * Provide assistance to managers in the development and implementation of Security Management arrangements and control strategies, including training, so as to ensure that they meet legislative requirements. |
|  |
| * Co-ordinate training needs analysis of security and emergency preparedness awareness across all levels of staff within the Trust to ensure needs are met. |
| * Liaise with the local NHS parties and local agencies as required. |

**5.6 Security Advisors**

It is the responsibility of the Security Advisors, as far as reasonably practicable to:

* Provide professional skills and expertise to tackle security management issues across a wide range of proactive and reactive tasks. The overall objective of the Security Advisor will be to work on behalf of SWYPFT to implement and maintain momentum in support of this policy.
* Ensuring that the Head of Safety, Security and Risk and SMD are fully aware of security issues which may affect the Trust, its staff, patients or the level of service for which it offers.
* Create a pro-security culture and raise security awareness.
* Offer support to staff involved in violence and aggression incident.
* Liaise with Police and other government agencies when required.

**5.7 Local Counter Fraud Specialist (LCFS)**

The LCFS will in line with the Trust Counter Fraud Policy:

* Ensure that the Director of Finance is informed about all referrals/cases and is provided with progress reports on all investigations.
* Be responsible for the day-to-day implementation of the seven generic areas of counter fraud, bribery and corruption activity and, in particular, the investigation of all suspicions of fraud
* Investigate all cases of fraud
* In consultation with the director of finance, report any case to the police or as agreed and in accordance with the *NHS Counter Fraud and Corruption Manual (counter fraud are still around, so keep in)*
* Ensure that other relevant parties are informed where necessary, e.g. Human Resources (HR) will be informed if an employee is the subject of a referral
* Ensure that South West Yorkshire Partnership NHS Foundation Trust‘s incident and losses reporting systems are followed
* Ensure that any system weaknesses identified as part of an investigation are followed up with management and reported to internal audit
* Adhere to the Counter Fraud Professional Accreditation Board (CFPAB)s Principles of Professional Conduct as set out in the *NHS Counter Fraud and Corruption Manual*
* Not have responsibility for or be in any way engaged in the management of security for any NHS body, but will liaise with the Security Advisor when appropriate.

**5.8 Human Resources Department Managers**

The Human Resources Department Managers are responsible for the production and maintenance of the Pre-Employment and Employment Checks, Appraisal and Performance Review and Leavers Policies. They are to ensure that Security Advisors are consulted to ensure effective personnel security measures are in place in each of these policies.

**5.9 Reducing Restrictive Physical Interventions (RRPI) Network Team Leader**

The RRPI team leader is responsible for the maintenance of RRPI training and Management of RRPI Policies and Guidance in close consultation with the Security Advisors. They also have to ensure that RRPI aspects of security incidents and personal safety are dealt with in the appropriate manner and raised at RRPI Trust Action Group (TAG).

**5.10 Specialist Advisors**

The Specialist Advisers are responsible for working with the Security Advisor to ensure that Health & Safety aspects of security incidents and personal safety are dealt with in the appropriate manner.

**5.11 Security Officers (Wakefield Based)**

Security Officers are responsible for managing operational security in line with the trust policy and is responsible for working with the Security Advisor to provide an environment that is safe and secure for all. The security officers are available for support during the hours of 8am to 6pm, Monday to Friday and based at Fieldhead.

Security Officers will receive reports on breaches of security and any offences in connection with crime or misconduct. They are to assist the Security Advisors and/or the Police with any investigation that is required as a result of theft, criminal damage and assault; as and when necessary. They are responsible for the maintenance of the physical security, CCTV and access control systems, security presence and day time patrols to various trust premises, in close consultation with the Security Advisors.

The security team can also offer a security presence at various trust premises, when required.

The security officers also support with car parking arrangements at Wakefield premises, but can also advise and support other locations where required.

**5.12 Contracted Security Service Provider**

The out of hours security service is provided by the Security Contractor under the specific contractual arrangements. The Security Service Provider is responsible for the operational security, key holding, alarm response and emergency response to various SWYPFT sites. The service level specification details the requirements of this service.

Security Services, where provided at other sites where SWYPFT operates clinical services are provided by the relevant landlord.

The Trust’s Security Advisors will liaise closely with the Security Services Provider(s) to ensure the aims of this Policy are achieved and that any incidents resulting in breaches of security are reviewed and lessons learnt addressed.

**5.13 All Managers and Employees**

Security is the responsibility of all managers and employees, and they are expected to co-operate with management to achieve the aims, objectives and principles of the security management policy. Great emphasis is placed on the importance of co-operation of all staff in observing security and combating crime.

Where staff know or suspect a breach in security, they must report it immediately via DATIX in accordance with the Incident Reporting Policy and when appropriate, to the Police.

**6. Process**

It is essential that the work undertaken by the Security Advisers meets national standards, to that end; SWYPFT continues to work within the now disbanded NHS Protect, standards and all relevant standards as defined by the Social Care Act 2012. As good practice, until further guidance/advice is forthcoming from NHS England.

Furthermore, the Trust will comply with all clauses set out within the NHS Standard contract as per Service Condition 24.

Security Advisors are required to:

* To implement and maintain appropriate security management arrangements (Service condition 24.1).
* To complete an annual Crime Profile within one month of contract commencement date (Service condition 24.2).
* Report and suspected fraud incidents to Local Counter Fraud Specialist (LCFS)
* Submit regular updates to the Safety and Resilience TAG on its work over the preceding quarter, including identifying developing trends/issues and progress with actions from the Work Plan.
* Submits an annual report that complies with the NHS Protect format to the Board through the Safety and Resilience TAG.
* Ensure that successfully obtained sanctions and redress are appropriately communicated via internal (Communications Department, Task Action Groups (TAGS)) or external media.

**7. Training Requirements**

7.1 SWYPFT recognises the need for effective training of staff to deal with security related issues and will, through the Learning and Development Department and the Security Advisor, ensure security advice and training, is provided with regard to:

* Management of Violence and Aggression to reduce the likelihood of assault.
* Conflict Resolution Training.
* Personal security and safety within the working environment.
* Responding promptly and effectively to all criminal events.

7.2 Specific areas where training is required will be identified in individual policies; however, these should include a minimum of:

* Conflict Resolution Training for all staff who interact with the public

* Physical Intervention and Assault Avoidance Skills (where required by risk assessment)
* Security/Crime Awareness
* Lone Working Safety (community based staff who conduct home visits)

**8. Sanctions**

There is a range of sanctions that can be applied to those who commit crimes against SWYPFT, whether they are patients, members of the public or staff. In terms of patients and the public, this primarily consists of criminal and civil law. When antisocial behaviour takes place in a healthcare setting, administrative action can also be considered, for example, withdrawal of treatment and removal from a practitioner’s list. For staff and professionals, disciplinary and professional regulatory processes may be appropriate in addition to criminal and civil sanctions.

**8.1 Criminal**

If matters are reported to the Police, the decision as to whether to progress a case lies with the Criminal Prosecution Service (CPS). However, there may be cases where the Police and the CPS have decided not to pursue a criminal prosecution and the Security Advisor and the SMD believe that this is not the right course of action. The Security Advisor should establish the reasons for the matter not being pursued. The Security Advisor should inform the Police of.

* The losses and costs incurred by the Trust (e.g. time off sick by staff, the cost of replacement staff or locum cover, the cost of replacing stolen or damaged property or assets).
* The losses and costs incurred by the individual (in the case of an assault).
* The impact of the incident on the delivery of healthcare in that community (e.g. number and type of appointments cancelled, any buildings that had to be closed, any healthcare professionals not able to carry out their jobs or leaving the health service entirely).

Not only does this serve to remind the court of the severity of the matter before them when they consider passing sentence, but it can also, if precise costs/amounts are known, allow them to award compensation for all or some of the costs incurred, including the cost of the investigation and prosecution in some circumstances. It also makes the court aware of the full cost of what may initially appear to be a minor incident.

**8.2 Civil Courts**

There are three main areas where SWYPFT may be involved with civil courts:

* Injunctions.
* Claims for compensation/damages.
* Personal injury.

**8.3 Civil Action**

This should be considered if injunctive or restraining powers are required to protect SWYPFT staff, property and assets in cases where the criminal process (including Anti-Social Behaviour Orders (ASBOs)) could take too long or would be inappropriate.

As with criminal cases, outcomes should be recorded on the Datix system, and the advanced warning system should be used. All costs should be recorded on the Datix System, including any awards made to SWYPFT by the civil courts.

**8.4 Injunctions**

An injunction is a court order that forbids a person from doing something, or that orders them to take certain action. An injunction could, for example, be sought to prevent someone from visiting certain premises or to prevent harassment.

Breach of an injunction is not a criminal offence, but it is a contempt of court. Proceedings for any breach would have to be taken by the party who obtained the injunction. The court has the power to fine or imprison a person for contempt of court. Some injunctions allow the Police to arrest the individual if they breach the terms of the injunction. An injunction only becomes valid once the person to whom it applies has been personally handed a copy.

**8.5 Claims for Compensation/Damages**

Civil courts can also rule on whether one party should make a payment to another. Such a claim could be made against an individual who has damaged SWYPFT property.

It is more cost-effective if the criminal court is asked to make a compensation order at the conclusion of criminal proceedings, but this is not always possible.

Before embarking on such a claim, it is important to consider whether the cost of the court action will outweigh the monies recovered and possible deterrent effect, and whether the individual concerned has the ability to pay.

**8.6 Personal Injury**

Personal damages claims are brought by individuals who have suffered some injury or loss as a result of the actions or negligence of another person or organisation. For example, a member of staff suing the person who has assaulted them for financial compensation for the injuries suffered.

**8.7 Hate Crime and Hate Incidents**

A hate crime is any criminal offence which is perceived by the victim or any other person, to be motivated by hostility or prejudice based on a person's disability, race, religion, sexual orientation or gender identity or perceived disability, race, religion, sexual orientation or gender identity.

Examples include:

* Physical attacks, such as physical assault, damage to property, offensive graffiti and arson.
* Threat of attack, such as inciting hatred by words, pictures or videos, offensive letters, abusive or obscene telephone calls, groups hanging around to intimidate, and unfounded malicious complaints.

A hate incident is any non-crime incident which is perceived by the victim or any other person to be motivated by hostility or prejudice based on a person's disability, race, religion, sexual orientation or gender identity or perceived disability, race, religion, sexual orientation or gender identity.

Examples include:

* Verbal or online abuse, insults or harassment, such as taunting, offensive leaflets and posters, abusive gestures, dumping of rubbish outside homes or through letterboxes, and bullying at school or in the workplace.
* A hate incident doesn't mean that we won't take it seriously if someone reports it.

The trust has a zero tolerance policy on abusive behaviour towards staff and will not hesitate to report hate crimes to the police.  Trust staff are encouraged to report any incidents of hate crime to management and the police.

The trust is committed to support staff who are victims or Hate crimes and/or incidents. The trust developed support through the Equity guardians who can support for frontline colleagues experiencing abuse. Our network of equity guardians gives advice and support to frontline colleagues who experience racist abuse from service users.

The Trust is committed to tackling hate crime and want to raise awareness of what a hate crime is and help people understand that it is not right to target individuals based on their identity. Some resources, including posters and guidance have been developed to support victims of hate crimes.

Hate crime not only harms its victims, but it also harms their families and communities.

**8.8**  **CBOs (Criminal Behaviour Orders) CPIs (Crime Prevention injunctions).**

CBOs and CPIs are civil orders that exist to protect the public from behaviour that caused or is likely to cause harassment, alarm or distress. An order contains conditions prohibiting the offender from specific antisocial acts or from entering defined areas and is effective for a minimum of two years. The orders are not criminal penalties and are not intended to punish the offender. They should not be viewed as an option of last resort.

The police will usually raise the possibility of an application for a CBO against an individual at the point of charge. A local authority may also approach the prosecution directly with a request to consider an application for a CBO without having to go via the police. The police / local authority must provide evidence to support the request for a CBO. Prosecutors should be alert at charging stage and beyond to cases in which a CBO application may be appropriate.

Before applying for a CBO for a youth, the prosecution must find out the view of the local youth offending team (YOT). In practice, the organisation preparing the application for the CBO (the police or local authority) will find out the view of YOT. If the views of YOT are not present on the file, the prosecutor must contact the police / local authority to request the information.

A CBO may be varied or discharged by the court which made the original order. Either the offender or the prosecution can make an application but if this is dismissed by the court, neither party can make a subsequent application without the consent of either the court or the other party.

It is a criminal offence if an offender fails to comply, without reasonable excuse, with the prohibitions and / or requirements in the CBO.

**9. Redress**

**9.1 Recovery**

Two principles lie behind effective recovery:

* Monies lost through security-related incidents and breaches can be returned to patient care.
* Recovery delivers an important deterrent message to staff, patients and the public: that crime does not pay and that SWYPFT will always pursue redress from those who attack it and deprive it of valuable resources.

There are a number of avenues through which to seek redress:

**9.1.1 Compensation Through the Criminal Courts**

Either as a sentence in its own right or in addition to another sentence imposed. The court may order a defendant to pay compensation to the victim(s) of their crime. Compensation orders are intended, however, to be used in straightforward cases where no great amount is at stake. They can be made in a number of cases, including (but not limited to) personal injury, loss and damage.

**9.1.2 Civil Action to Obtain a Civil Remedy**

A civil remedy may be granted by a court to a party to a civil action. It may include (but is not limited to) the common law remedy of damages (a sum of money awarded by a court to compensate a claimant for their losses) or an injunction (a remedy in the form of a court order addressed to a particular person, that either prohibits them from doing or continuing to do a certain act or orders them to do a certain act)

**9.1.3 Confiscation Order**

An order that requires an offender convicted of an offence that has benefited from that offence to pay a sum that the court considers appropriate. These are intended to be used in more complex and difficult cases where a substantial amount of money is at stake.

**9.2 Decision on Redress**

The Security Advisor will decide along with the Deputy Director of Finance and the relevant Service Deputy Director if redress is suitable. Advice will also be sought from the ASMS. If at any point any party feels that the Redress process needs assistance or is not being taken forwards as appropriate the SMD is to be contacted.

**9.3 Communications of prosecutions**

Where appropriate, the trust will publicise successful prosecutions of cases relating to a) denying unnecessary access to premises b) the consequences of assaulting NHS staff c) breaching the security of NHS premises and property d) acts of theft and criminal damage.

It is accepted that due to the nature of the organisation that this will be done on a case by case basis and it should follow an agreed communications strategy with the victim/s of the specific crime.

**10. Development process**

**10.1 Identification of Need**

The policy has been developed to ensure Security Industry good practice and in line with historic NHS Protect Standards and guidance as per the Standards for Providers.

**10.2 Stakeholder Involvement**

Consultation with relevant stakeholders secures ‘buy in’ and provides an opportunity to identify and eliminate potential barriers to implementation.

The lead director is responsible for ensuring relevant stakeholders have been consulted during the development of the policy. The following individuals or groups have been consulted with:

| **Stakeholder** | **Level of involvement** |
| --- | --- |
| Executive Management Team | Approval – (may also be involved at the outset in confirming the requirement for a new policy or agreeing the development process) |
| Directors | Initiation, lead, development, receipt, circulation |
| Business Delivery Units (BDUs) | Development, consultation, dissemination, implementation, monitoring |
| Specialist Advisors | Development, consultation, dissemination, implementation |
| Service user and carers | Development, consultation |
| Trust Action Groups | Development, consultation, dissemination, implementation |
| Staff side | Development, consultation, dissemination |
| Police | Development, consultation |

**10.3 Equality Impact Assessment**

The Trust aims to ensure its policies and procedures promote equality both as a provider of services and as an employer. All new policies and procedures should be subject to an Equality Impact Assessment. A tool to support this process is included at appendix B to this document.

**11. Approval and ratification process**

The Policy will be approved by EMT after initial development and consultation process by BDU’s and appropriate TAG’s as identified in stakeholder involvement.

**12. Process for review**

The policy will be reviewed every three years from the approval date. This may be brought forward if earlier review is required, for example because of an identified risk or change in national policy.

If no amendment is required, this should be reported to the Executive Management Team or Trust Board for ratification by the review date and the policy will be reissued.

An Equality Impact Assessment (EIA) for this policy has been completed as it has not previously been subject to EIA.

**13. References**

This document has been developed in line with guidance issued by the NHS Protect and it should be read in conjunction with

* Violence at Work Policy.
* ​Reducing restrictive physical interventions Policy and Guidance
* Safe and Secure Environment Policy
* Lone Worker Policy
* Health & Safety Policy
* Supporting Staff Policy
* Police Liaison Policy
* NHS Violence Reduction Standards
* Procedure for Reporting of Violent and Anti-social Offending
* NHS Standard Contract 2021

**14. Dissemination**

Once approved, the Security Advisor will be responsible for ensuring the updated version is added to the document store on the intranet and is included in the staff brief.

The integrated governance manager is responsible for ensuring the document being replaced is removed from the document store and that an electronic copy, clearly marked with version details, is retained as a corporate record.

If local teams download and keep a paper version of procedural documents, the manager must identify someone within the team who is responsible for updating the paper version when a policy change is communicated via the weekly Comms.

**15. Implementation**

All policies and procedures must identify the arrangements for implementation, including:

* any training requirements, including which staff groups this affects and the arrangements and timescale for delivering training.
* any resource requirements, including staff, and how these will be met.
* support available to assist implementation.
* arrangements for ensuring the policy or procedure is being followed.
* monitoring and audit arrangements.

**16. Monitoring Compliance with the Policy**

This policy will be monitored for compliance and reviewed within Security Advisors workplans and NHS Violence Reductions Standards. The trust needs to complete an annual Self Review Toolkit (SRT) to ensure compliance with NHS Violence Reduction standards.

Methods to monitor include:

* monitoring and analysis of incidents, performance reports and training records.
* Annual H&S monitoring audit.
* Security risk assessments.
* monitoring of delivery of actions plans via Safety and ResilienceTAG.
* Completion of the Violence reduction toolkit.

**Appendix A –**

**Version Control Sheet**

*This sheet should provide a history of previous versions of the policy and changes made*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Status** | **Comment / changes** |
| 1 | March 2015 | Johan Celliers | Draft 1 | Draft 1 – completed and circulated for first consultation. |
| 2 | April 2015 | Johan Celliers | Draft 2 | Draft 2 – review of content and further circulation for comment. |
| 3 | June 2015 | Johan Celliers | Draft 3 | Draft 3 Emma Hilton/Martin Brandon comments included |
| 4 | July 2015 | Johan Celliers | Draft 4 | Draft 4 Emma Hilton update |
| 5 | September 2015 | Johan Celliers | Draft 5 -8 | Circulated for consultation and comments to members H&S subgroups and H&S and Emergency Preparedness TAG – updated with comments |
| 6 | October 2015 | Johan Celliers | Draft 8 | Approvals EMT |
| 7 | Jan 2019 | John Sanderson | Draft 9 | Approvals EMT |
| 8 | Dec 2021 | Johan Celliers | Draft 10 | Approvals EMT – remove all references to LSMS and NHS Protect. Updated roles and Responsibilities section due to Executive Management changes. |
| 9 | Jan22 | Johan Celliers | Draft 11 | Updated references to roles and titles, removed and updated references to Violence and aggression, updated cover page, updated compliance section, added Hate Crime section. |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Appendix B**

**Equality Impact Assessment template**

**to be completed for all policies, procedures and strategies**

**Date of EIA: 14/12/2021 Review Date: December 2024**

**Completed By: Johan Celliers**

|  |  |  |
| --- | --- | --- |
|  | **QUESTIONS** | **ANSWERS AND ACTIONS** |
| **1** | **What is being assessed?**  Prompt: what is the function of this document (new or revised) | Security Management Policy2022 |
| **2** | **Description of the document**  Prompt: What is the aim of this document | The Security Management Policy document aims to provide guidance on the developing and implementation of the trust’s security strategy to protect staff and trust assets, so that it can provide high quality healthcare to the public and take all practicable steps to protect the property of our patients while they are admitted to our care. |
| **3** | **Lead contact person for the Equality Impact Assessment** | Johan Celliers, Security Advisor |
| **4** | **Who else is involved in undertaking this Equality Impact Assessment** | Aboobaker Bhana, Equality and Involvement Manager |
| **5** | **Sources of information used to identify barriers etc**  Prompts: service delivery equality data – refer to equality dashboards ([BI Reporting - Home (sharepoint.com)](https://swyt.sharepoint.com/sites/BIReporting) satisfaction surveys, complaints, local demographics, national or local research & statistics, anecdotal. Contact [InvolvingPeople@swyt.nhs.uk](mailto:InvolvingPeople@swyt.nhs.uk) for insight  **What does your research tell you about the impact your proposal will have on the following equality groups?** | **Workforce data**  As per workforce annual report 2020   * The Trust currently employs 4,328 staff delivering a range of services including mental health, learning disability, forensic, physical health and an extensive range of community services. * The number of staff who have not stated their religious belief (Unknown) has decreased slightly from 2018 (23%) to just below 21% currently. Staff reported as 48% Christianity, 3%Islam, 12% other and 17% Atheism. * There has been a significant increase in the number of staff reporting their religion and sexual orientation. Currently 83% of staff have provided data indicating their sexual orientation, which is a slight improvement on last year’s figures. |
| **5a** | **Disability Groups:**  Prompt: Learning Disabilities or  Difficulties, Physical, Visual, Hearing  disabilities and people with long term  conditions such Diabetes, Cancer,  Stroke, Heart Disease etc. Accessible  information standard | * The Workforce data shows that 6.1% of our staff considerthemselves to have a disability, the same figure as last year. The total number of staff is 266, this is an increase of 11 since last year. |
|  | **QUESTIONS** | **ANSWERS AND ACTIONS** |
| **5b** | **Gender:**  Prompt: Female & Male issues should be considered | * The Trust split of 77.9% female to 22.1% male is reflected approximately across most areas, except for Medical Staff (36%/64%). As in previous years, female staff make up over three quarters of Trust staff. |
| **5c** | **Age:**  Prompt: Older people & Young People issues should be considered | * As in previous years, the highest number of Trust staff fall in the age bands 40-49 and 50-59 with over 55% of the total staff being between 40 and 59. Just over 42% of medical staff are between 40 and 49. Support Services have the highest percentage of staff in the 60-69 age bands with 14% (102) being 60 or over |
| **5d** | **Sexual Orientation:**  Prompt: Heterosexual, Bisexual, Gay,  Lesbian groups are included in this  Category | * There has been a significant increase in the number of staff reporting their religion and sexual orientation. Currently 83% of staff have provided data indicating their sexual orientation, which is a slight improvement on last year’s figures. The policy provides some specific guidance on Hate Crimes that could be directed to this group of staff. |
| **5e** | **Religion & Belief:**  Prompt: Main faith groups and people with no belief or philosophical belief issues should be considered | * There has been a significant increase in the number of staff reporting their religion and sexual orientation. Currently 83% of staff have provided data indicating their sexual orientation, which is a slight improvement on last year’s figures. They all face the same potential impacts (both positive and negative from climatic & environment changes. |
| **5f** | **Marriage and Civil Partnership**  Prompt: Single, Married, Co-habiting, Widowed, Civil Partnership status are included in this category | * People who are Single, Married, Co-habiting, Widowed or in a Civil Partnership all face the same potential impacts (both positive and negative) from security and safety incidents. |
| **5g** | **Pregnancy and Maternity**  Prompt: Currently pregnant or have been pregnant in the last 12 months should be considered | * Females who are currently pregnant or have been pregnant in the last 12 months and their offspring all face the same potential impacts (both positive and negative) from security and safety incidents |
| **5h** | **Gender Re-assignment**  Prompt: Transgender issues should be considered | * People who are currently pregnant or have been pregnant in the last 12 months and their offspring all face the same potential impacts (both positive and negative) from security and safety incidents |
| **5I** | **Carers**  Prompt: Caring responsibilities paid or unpaid, hours this is done should be considered | * Carers and their dependants all face the same potential impacts (both positive and negative) from security and safety incidents |
| **5j** | **Race**  Prompt: Indigenous population and BME Groups such as Black African and Caribbean, Mixed Heritage, South Asian, Chinese, Irish, new Migrant, Asylum & Refugee, Gypsy & Travelling communities.) | * The Trusts staff profile has a larger White British representation than the local demographic of the people that it serves collectively. Trust wide, 90% of the total staff in post are white British which is similar to previous years and equates to an over-representation of 1.3% (last year 1.1%). Mixed race staff are underrepresented by 0.2%, Chinese staff are over-represented by 0.2%, Black staff are over-represented by 1.6% and South Asian staff are under-represented by 3.2%. However, the Trust’s local demographic has large variation in BAME representation and there is a significant under-representation of South Asian staff in Kirklees/Calderdale (exact figures not available due to mixed teams). The Policy provide guidance on Hate Crimes that could potentially affect staff from these groups. |

**Action Plan**

EIAs are now reviewed using a grading approach which is in line with our Equality Delivery System (EDS). This rates the quality of the EIA. This means that the team can review the EIA and make recommendations only. The rating and suggested standards are set out below:

* + **Under-developed** – red – **No data**. **No strands** of equality
  + **Developing** – amber – **Some census data plus workforce**. **Two strands** of equality addressed
  + **Achieving** – green – **Some census data plus workforce. Five strands** of equality addressed
  + **Excelling** – purple –**All the data and all the strands** addressed

Potential themes for actions: Geographical location, built environment, timing, costs of the service, make up of your workforce, stereotypes and assumptions, equality monitoring, community relations/cohesion, same sex wards and care, specific issues/barriers.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Who will benefit from this action?** | **Tick all that apply** | **Action 1:**  **This is what we are going to do** | **Action 2:**  **This is what we are going to do** | **Action 3:**  **This is what we are going to do** | **Lead/s** | **By When** | **Update/review outcome** | **RAG** |
| Age, Disability,  Gender reassignment,  Marriage and/or civil partnership,  Race, Religion or belief, Sex, Sexual orientation  Pregnancy and maternity or Carers | **✓** | The Trust will ensure that people of all backgrounds, identities and ages in their present circumstance will not suffer from any negative security and safety impact, where the Trust directly affects the local outcome from its care activities | Individuals will be encouraged and empowered to raise awareness and request security and safety changes in their workplace where this supports effective service delivery. | Involve the various groups & support networks, i.e., LGBT+, BAME, Disability etc to ensure there continue to be no unintended consequences to individuals from the Security Management Policy 2022 | Johan Celliers | February 2025 | February 2025 | **Developing** |

**Involvement & Consultation: New or Previous (please include any evidence of activity undertaken in the box below)**

|  |
| --- |
| An integral element of the Security Management Policy 2022 Equality Impact Assessment is to involve the various groups & support networks, i.e., LGBT+, BAME, Disability etc to ensure there continue to be no unintended consequences to individuals from Trust environmental impacts |

|  |
| --- |
| 1. **Methods of Monitoring progress on Actions**   Feedback of Monitoring progress on Actions will be through feedback (positive & negative) from the various groups & support networks, i.e., LGBT+, BAME, Disability etc |

|  |
| --- |
| 1. **Publishing the Equality Impact Assessment**   The Equality Impact Assessment has been published as an integral part of the Security Management Policy 2022. This is available on the Trust intranet & via Freedom of Information requests |

|  |
| --- |
| 1. **Signing off Equality Impact Assessment:**   Security Management Policy 2022 Equality Impact Assessment has been signed off by Nick Phillips, Associate Director of Estates and Facilities South West Yorkshire Partnerships Foundation Trust |

|  |
| --- |
|  |

|  |
| --- |
|  |

***Once approved, you must forward a copy of this***

***Assessment/Action Plan by email to:***

[**InvolvingPeople@swyt.nhs.uk**](mailto:InvolvingPeople@swyt.nhs.uk)

**Please note that the EIA is a public document and will be published on the web.**

**Failing to complete an EIA could expose the Trust to future legal challenge**

**Appendix C - Checklist for the Review and Approval of Procedural Document**

*To be completed and attached to any policy document when submitted to EMT for consideration and approval.*

|  | **Title of document being reviewed:** | **Yes/No/ Unsure** | **Comments** |
| --- | --- | --- | --- |
| **1.** | **Title** |  |  |
|  | Is the title clear and unambiguous? | YES |  |
|  | Is it clear whether the document is a guideline, policy, protocol or standard? | YES |  |
|  | Is it clear in the introduction whether this document replaces or supersedes a previous document? | YES |  |
| **2.** | **Rationale** |  |  |
|  | Are reasons for development of the document stated? | YES |  |
| **3.** | **Development Process** |  |  |
|  | Is the method described in brief? | YES |  |
|  | Are people involved in the development identified? | YES |  |
|  | Do you feel a reasonable attempt has been made to ensure relevant expertise has been used? | YES |  |
|  | Is there evidence of consultation with stakeholders and users? | EMT |  |
| **4.** | **Content** |  |  |
|  | Is the objective of the document clear? | YES |  |
|  | Is the target population clear and unambiguous? | YES |  |
|  | Are the intended outcomes described? | YES |  |
|  | Are the statements clear and unambiguous? | YES |  |
| **5.** | **Evidence Base** |  |  |
|  | Is the type of evidence to support the document identified explicitly? | YES |  |
|  | Are key references cited? | YES |  |
|  | Are the references cited in full? | YES |  |
|  | Are supporting documents referenced? | YES |  |
| **6.** | **Approval** |  |  |
|  | Does the document identify which committee/group will approve it? | YES |  |
|  | If appropriate have the joint Human Resources/staff side committee (or equivalent) approved the document? | N/A |  |
| **7.** | **Dissemination and Implementation** |  |  |
|  | Is there an outline/plan to identify how this will be done? | YES |  |
|  | Does the plan include the necessary training/support to ensure compliance? | N/A |  |
| **8.** | **Document Control** |  |  |
|  | Does the document identify where it will be held? | YES |  |
|  | Have archiving arrangements for superseded documents been addressed? | YES |  |
| **9.** | **Process to Monitor Compliance and Effectiveness** |  |  |
|  | Are there measurable standards or KPIs to support the monitoring of compliance with and effectiveness of the document? | YES |  |
|  | Is there a plan to review or audit compliance with the document? | YES |  |
| **10.** | **Review Date** |  |  |
|  | Is the review date identified? | YES |  |
|  | Is the frequency of review identified? If so is it acceptable? | YES |  |
| **11.** | **Overall Responsibility for the Document** |  |  |
|  | Is it clear who will be responsible implementation and review of the document? | YES |  |