NHS
South West
Yorkshire Partnership
NHS Foundation Trust

Document name:	Safe & Secure Environment Policy (779)
Document type:	Policy
What does this policy replace?	Review and update on previous version of policy
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:	September 2020
Next review:	September 2024
Approved by:	Executive Management Team
Developed by:	Security Adviser
Director leads:	Executive director of finance, estates and resources
Contact for advice:	Security Adviser

Contents

SAFE AND SECURE ENVIRONMENT POLICY

1. Introduction

Safe and secure environments within the Trust are concerned with the provision of safeguards to protect the safety of those who visit or work within Trust premises and the protection of property belonging to service users, visitors, staff and the Trust.

Security is the responsibility of all staff not only in safeguarding their own well-being, but that of service users, visitors and colleagues. It is also the responsibility of all staff to safeguard the property and assets of all service users, visitors, colleagues and the Trust.

2. Purpose

The policy of the Trust is to ensure a safe and secure environment as far as reasonably practicable in the workplace, and to promote the health and safety of staff, service users, visitors or others. This policy document, whilst primarily designed to ensure the safety of staff working in the Trust, also provides for how situations are dealt with in a way that minimises the risk to users and visitors

2.1 Scope of the policy

This policy applies to all employees including contractors and employees of other organisations on site and volunteers. Any breach of this policy may lead to disciplinary and/or legal action.

The primary objectives being:

- Protection of life from malicious criminal activity or other hazard;
- Protection of a healthy living/working environment from malicious criminal activity or other hazard;
- Protection of service users and staff from verbal or physical abuse/assault;
- Prevention of the loss of service users', visitors' and Trust property because of criminal activity;
- Protection of Trust property against malicious acts, theft, criminal damage, trespass, etc.
- Preservation of good order within the Trust's premises;
- Detection, reporting of suspected offenders committing offences against service users, visitor, staff, Trust or private property within the Trust's premises;
- Maintenance of the excellent public perception of the Trust.

2.2 Rationale for development

The Trust aims to balance the rights and responsibilities of people using its services with those of employees, with a clear approach to health & safety risk management. It also aims to support staff, by ensuring that working environments which are controlled by the Trust are as safe and pleasant to work in as possible.

Safe environments are essential to healthcare provision to ensure staff, Trust partners, service users, visitors and contractors are protected from incidents, accidents, injury and disease as far as reasonably practicable and to provide a safe place in which high quality clinical care is provided. During visits to the Trust stakeholders have a right to have their needs assessed and action taken so they are protected from harm. When adverse incidents occur, appropriate responses should be taken to support individuals

This document outlines how these aims will be addressed and indicates the Trust's responsibilities and those of its staff. Risks from working environments will be assessed by use of the Trust recognised risk assessments (clinical and non-clinical) in order to develop safe and supportive systems as well as working environments.

2.3 Objectives and intended outcome of the policy

The intended outcome of this policy is to provide the Trust and Trust staff with the knowledge and skills to effectively reduce and manage the risk from adverse risks in the workplace.

The objectives are to:

- Maintain and improve working environments to ensure, as far as reasonably practicable, a safe and secure working environment.
- Identify who is responsible for a local safe and secure working environment within the Trust, the remit and scope of their roles
- State the Trust's commitment to improve working environments to ensure, as far as reasonably practicable, a safe and secure working environment for service users, staff and visitors
- Ensure SWYPFT employees are aware of, and can access mechanisms to maintain and improve working environments as far as reasonably practicable

3. Roles and Responsibilities

The following duties apply to this policy.

3.1 Trust Board

The Trust Board will ensure, so far as is reasonably practicable, that all steps are taken to ensure secure and safe environments for all stakeholders including, staff, partners, service users, visitors and others.

3.2 The Chief Executive

The Chief Executive is ultimately responsible for the overall health and safety in the Trust, including secure and safe environments. The Chief Executive will ensure that all Directors, Assistant Directors, Senior Managers and staff, understand and accept their rights and responsibilities for health and safety at work and the implementation of the Trust's Health & Safety Policies.

3.3 Director of Human Resources, Organisational Development and Estates

The Director of Human Resources, Organisational Development and Estates has lead responsibility and delegates management of secure and safe environments to the Facilities Department, who lead with the assistance of Business Delivery Units and other departments with the planning, control and implementation of security measures.

3.4 Directors

Every Director carries the responsibility for ensuring that within their sphere of responsibility, appropriate risk assessments have been undertaken and that there are adequate local working procedures to ensure secure and safe environments.

Directors will disseminate health & safety risk assessments for completion to individual service areas or departments to ensure individual Risk Assessment folders for each service area or department are compiled, as appropriate, and are made available for staff whilst they are on duty.

3.5 Deputy Directors, General, Service & Line Managers

Deputy Directors, General, Service and Line Managers are responsible for managing and ensuring, as far as reasonably practicable, secure and safe environments within their area of responsibility, under the authority of their director and will comply with all Trust health & safety requirements. General, Service and Line Managers will ensure employees are aware of their rights and responsibilities for the provision and maintenance of a safe and healthy environment for staff, service users and visitors. This will be done by providing all employees with information, instruction, training and/or supervision as appropriate to their needs so that they can work safely and understand their obligations under the Health & Safety at Work Act 1974 and associated legislation.

Heads of individual departments, Directorates and Business Delivery Units are responsible for the day to day security of their working areas and the implementation of Trust security procedures. This includes undertaking and reviewing annually (or whenever changes in working practices or processes occur) local risk assessments relating to the physical security and assets of their premises. Advice should always be sought in the first instance through Facilities at Fieldhead.

Heads of Department must ensure staff report all breaches of security, criminal activity, incidents, or suspicions to security services in the area where they work immediately. Following an incident, a Trust incident reporting form should be completed and input onto the Trust's DATIX incident reporting system.

3.6 Safety & Resilience TAG

The Director of Human Resources, Organisational Development and Estates delegates the responsibility and management of Secure and Safe Environments Policy to the Safety & Resilience TAG.

Security Incidents and concerns around safe working environments are reviewed and monitored through the Safety & Resilience TAG. The Safety & Resilience TAG assesses reports from all service areas, analyses incidents, investigate trends, complete a trust wide action plan and develops work streams to act on those trends.

Organisational action plans, following the annual health & safety monitoring programme will similarly be evaluated and discussed as necessary by the Safety & Resilience TAG as part of the overall risk assessment on securing local secure and safe environments.

3.7 Trust Local Security Management Specialists (LSMS)/Security Advisor

The overall objective of the LSMS's is to deliver an environment that is safe and secure so that the highest standards of clinical care can be made available to service users.

The objective will be achieved by working in close partnership with stakeholders within the NHS and external organisations such as the Police, professional representative bodies, and trade unions. The LSMS's will aim to provide a comprehensive, inclusive and professional security management service for the Trust and work towards the creation of a pro-security management culture.

3.8 Trust Specialist Advisers

In order to assist the Chief Executive and Directors discharge their health, safety and welfare responsibilities and to meet its obligations under the requirements of the Health and Safety at Work Act 1974 and other associated health & safety legislation, the Trust will ensure it has access to such numbers of health & safety and other advisers as is reasonable and appropriate. Such Advisers will be designated as competent in line with the requirements of these regulations. They will be available to offer advice, guidance and support to Directors, Managers and Staff, who all have responsibility to either implement advice provided up to their level of authority or if not record the reason(s) why and share this with the management team concerned and the relevant competent adviser for further consideration.

3.9 Employee Responsibilities

Employees of the Trust have responsibility for:

- Ensuring that effective measures are taken to ensure that Trust premises and property are maintained in a secure condition;
- Taking steps to safeguard against loss of Trust property and the property of individuals as far as reasonably practicable;
- Complying with all Trust policies and procedures;

- Taking reasonable steps to ensure their own personal security and that of colleagues and service users;
- Taking all reasonable steps to ensure security of their own personal possessions – the Trust takes no responsibility for personal possessions except in specific circumstances where personal property is handed to staff for safe keeping.

Every Trust employee, whilst having a right to a safe working environment, carries responsibility for their own health and safety and the safety of others. All staff are required to comply with Trust policies and procedures relating to health and safety matters.

Ultimately security is the responsibility of all personnel employed or acting on behalf of the Trust.

3.10 Facilities Department

The Facilities Department and the various security services are, with the help of Business Delivery Units and other teams, responsible for the day to day enforcement of security at all Trust premises. All heads of department, Directorates and local management teams should co-operate fully with Facilities/Security Services and ensure they are given all the necessary co-operation to carry out these duties.

3.11 Remit of Security Services

Security Services have the initial lead in investigation and detection of crime and security incidents within the Trust's business area. These investigations will on occasions be carried out in conjunction with Senior Management, Internal Audit or the Police. Where investigations are being carried out, it is imperative all staff co-operate with the Security Services, Internal Audit personnel or Police officers as appropriate.

Security Services are responsible for:

- Providing an operational security service for staff, service users and visitors within the Trust.
- Assisting with crime prevention/security training for staff.
- Recording and reporting promptly to Facilities all incidents of crime and security matters reported to or detected by the Security Services.
- Maintaining at all times liaison with Facilities, Police and other relevant bodies represented within the Trust's premises.
- Assisting with crime prevention programmes and campaigns to raise the profile of security and highlight the need for constant vigilance.
- Providing a service to escort staff from their areas of work, when reasonable, to other areas of the hospital or their vehicles.
- Assist the LSMS with risk assessment of trust premises and updating the risk assessment folder on a continuous basis.

4. Monitoring compliance with the policy

The Trust is required to ensure safe and secure environments. This include the assessment of risks in individual areas and departments in terms of providing safe and secure environments that are undertaken locally as stated in section five of this policy document.

Compliance with the safe and secure environment (security) policy will be monitored in the following ways:

- The Safety & Resilience TAG will analyse statistical evidence of weaknesses identified in working environments from DATIX every three months.
- Completed returns, by local managers, from the annual health & safety monitoring forms will be analysed by the clinical governance support team and presented to the Safety & Resilience TAG for discussion.
- The Safety & Resilience TAG will identify and agree an audit programme based on statistical information from DATIX and analysis of the annual monitoring return
- The Director of Human Resources, Organisational Development and Estates will present the Annual Safety Services Report to the Executive Management Team which contains annual security related data.

4.1 Specific Monitoring Responsibilities

The Trust Security and Logistics Officer has been authorised to support and assess individual services' performance against Trust specified objectives and targets in order to ensure that they are realistic; achievable and measurable. Such support and assessment is to encourage consistency and continuous improvement any concerns will be raised with the Health & Safety Manager for guidance.

In the absence of action by Directors and/or managers and after appropriate consultation, the Health and Safety Manager is empowered to advise the Chief Executive and/or the Trust Board that they should stop any activities on Trust owned, leased or shared property, if in their opinion it gives rise to imminent risk of serious personal injury. In the event of a decision to cease such activities, they will not be allowed to restart until such time as the cause of the danger is removed or rectified.

4.2 Managing Safe & Secure Work Environments Guidance for staff

Managing Safe & Secure Working Environments guidance is provided for staff to have an appreciation and understanding of the broad spectrum of issues relating to the

management of Safe & Secure Work Environments. This guidance is to supplement the training and advice provided relating to specific individual issues available from specialist advisors.

4.8 Methodology

The Clinical Governance and Clinical Safety Committee are responsible for scrutiny of this process.

4.9 Trust Wide Action Plan for Improvements

Improvements in the workplace to ensure safer and/or upgraded secure environments will be subject to capital bids from BDU's via the Estates TAG. Revised working practices as identified locally by BDU management teams or organisationally by relevant Specialist Advisers will be implemented after informing relevant staff and updating risk assessments. Security Risk Assessment or Crime Reduction Surveys are also completed on a rolling program. Any areas identified within the surveys can be put forward for capital funding via Estates TAG

5. Local Security Information to support Safe and Secure Environments

5.1 Cash Handling

When cash is moved, it should be done strictly in accordance with the policies incorporated and set out within Standing Financial Instructions. The following guidelines should be adhered to at all times:

- Movement of cash should be subject to security survey instructions laid down by the Security Adviser, in liaison with Finance Department.

- Defined instructions regarding the security of premises where cash is held will be adhered to as advised by the Security Adviser in liaison with Finance Department. All guidelines set out, will be the responsibility of the Director of Finance, who will review the policies from time to time in conjunction with the Local Security Management Specialist/Security Adviser

- Petty cash must be held in a secure place and records must be kept to demonstrate that any use of petty cash conforms to SWYPFT financial standing instructions, guidance and procedures. Local procedures must be developed to support the security of petty cash.

- A third party Cash In Transit (CIT) contractor will be delivering petty cash and patient money around the trust on weekly basis to specifically agreed locations.

- Any additional and special request for deliveries must be agreed by Finance and the Local Security Management Specialist.

5.2 Traffic & motor vehicle security

All motor vehicles used by staff, visitors and other external agencies should only park in an authorised parking area, which has been provided and authorised by the Trust. Vehicles and their contents are left on Trust property at the owners' own risk.

The Trust may issue parking permits which should be displayed at all times. However, this does not guarantee the permit holder a space. The Trust reserves the right to remove at the owner's expense any vehicle parked inappropriately on its premises.

The Trust reserves the right to take disciplinary action against members of staff, who persistently ignore warnings against inconsiderate or inappropriate parking, in line with guidance in Parking and On Site Traffic Policy

Any occurrences regarding traffic related incidents, theft, criminal damage or other offences should be reported immediately to security and recorded on the Trust's DATIX incident reporting system.

It should be noted that the whole of each site is private in relation to the entry and movement of vehicles. The Trust reserves the right to deny any vehicle access to any site, and to require drivers to conform to designated traffic regulations.

No obstructions will be permitted to fire exits, loading/unloading areas, client drop off points, pavements, or other service areas.

5.3 Pharmaceuticals

The Trust will take positive steps to protect all pharmaceuticals, by keeping them in secure cupboards. Not all pharmaceuticals are attractive to criminals, although of course, many are. Blank prescription forms will also be given physical protection against unauthorised access.
The following legislation now applies to the NHS.

- The Mis-use of Drugs Act 1971.
- The Mis-use of Drugs Safe Custody Regulations 1973.
- The Mis-use of Drugs Notification and Supply to Addicts Regulations 1973.
- The Medicines Act 1968.
- The Hazardous Waste (England and Wales) Regulations 2005
- Environmental Protection Act 1990
- Environment Act 1995

Guidelines on Safe and Secure Handling of pharmaceuticals.

The Trust, in developing the security policy, will take into account the recommendations of the 1988 Duthie Report by a Joint Sub-Committee of the Standing Medical, Nursery, Midwifery and Pharmaceutical Advisory Committee.

The Senior Chief Pharmacist should consult with Local Security Management Specialist, who are responsible for security in the Trust and will have an overall responsibility for security matters. This will assist in the process of monitoring progress and reaching the desired standards.

The Trust will maintain an effective system for ensuring that medicines are stored and handled safely and securely. Particular attention will be paid to methods of ordering, delivery and receiving pharmaceuticals. This will be detailed in the Medicines Code which is written by the Drug and Therapeutics Committee and approved by EMT

At each stage where pharmaceuticals change hands, there will be clearly laid down procedures defining where responsibilities lay, records to be kept and how often reconciliation of stocks are undertaken. These will be detailed in the Medicines Code.

Any discrepancies or missing Controlled Drugs or Prescription Forms must be reported to the applicable CCG's Pharmaceutical Representative the trust's Accountable Officer for Controlled Drugs (CDAO). The Senior Chief Pharmacist/CDAO must agree an appropriate process to manage the missing medication or prescription forms with input from the CCG NHS England Local Area Team (LAT). The incident might also require reporting to the Local Intelligence Network (LIN) for further support and information sharing.

5.4 Information

All staff and agents of the Trust taking up employment or work placements of any kind will understand the importance of ensuring client and Trust security information remains confidential, particularly in realms of helping to ensure safe and secure environments. It is incumbent upon all personnel in the recruitment chain to ensure individuals are made aware of the fact.

Everyone working in the NHS has a duty to keep information about you confidential. At the Trust this includes information recorded during interviews, meetings and supervision, information kept on our computer systems and any paper records held to in relation to your employment. All our staff and premises are subject to the same data protection and confidentiality measures.

Personal information collected and used by the NHS is controlled by the General Data Protection Regulation (GDPR). The GDPR includes six data protection principles: one of these is that information must be used lawfully, fairly and transparently: this means you have a right to know how we intend to use the information you provide. It also means you have a right to privacy that is respected through any use of your personal information by the NHS. Further information on the GDPR can be obtained from:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
SK9 5AF
Tel: 0303 123 1113 (local rate) or 01625 545745 (national rate)
https://ico.org.uk/

If you are concerned about how the Trust is using your personal information you have a right to complain to the Information Commissioner's Office.

The code of practice for disposal of confidential waste should be complied with under the terms of the policy that are in situ at all times and such waste must never be left unattended or insecure in the working environment

Particular care must always be taken with obsolete I.T. equipment that sensitive information is not left on floppy discs, hard drives or any other recording media. Always ask for advice from colleagues in the I.T. Department under such circumstances.

5.5 Contacting Police

Where a member of staff is witnessing a criminal act or reasonably believes that a criminal act is imminently likely to occur, the Police should be contacted immediately. Staff are encouraged to appropriately report all incidents of violence and aggression,

Where a Senior Departmental Manager feels the need to notify the police direct, appropriate Datix Report must be submitted as soon as possible.

Security Services will report all thefts, criminal damage or threats against the Trust and record the crime number issued by Police for individual incidents.

If **private** property has been stolen or damaged, it is the **owner's responsibility**, to contact the police.

Further advice can be sought from the trust Security Adviser.

5.6 Lockdown

Lockdown is the process of controlling the movement and access, both entry and exit, of people (NHS staff, service users and visitors) around a trust site or other specific trust building/area in response to an identified risk, threat or hazard that might impact upon the security of service users, staff and assets or, indeed, the capacity of that facility to continue to operate. A lockdown is achieved through a combination of physical security measures and the deployment of security personnel.

Senior Service Management must ensure that Lockdown Risk Profiles in the Appendices are completes for all Trust premises occupied by their services. The Profiles must be reviewed every three years.

For further information please refer to The Trust Lockdown Policy available on the Intranet and Health and Safety Policy Manuals.

5.7 Access control (FOBs), keys and locks

Keys, access control fobs should be secure and should only be made available to bona fide NHS staff. Local procedures and systems should be in place to ensure that

appropriate records are kept of the whereabouts of keys and fobs that are available for use by a number of different staff.

Any lost keys or fobs should be reported as soon as possible to the unit manager and estates/security department. The Trust has the right to keep access activity data of individual fobs and to access and utilise the data appropriately when required.

Staff, who are allocated a fob, must take note that fob usage and movement are recorded on the access control database for appropriate and obvious security reasons. If required, the access control database can be accessed to support security related or other internal investigations.

5.8 Alerts

The purpose of Security Management Alerts is to notify the NHS Trust of security related issues which may pose a significant present or potential threat to NHS staff.

Alerts are one element of security management work to protect NHS Staff and to ensure security of Trust resources. The alerts form part of the trust strategic approach to detection, prevention investigation and taking appropriate action when threats are identified.

The Local Security Management specialist will disseminate alerts appropriately as guided by the local partnerships and security management working groups.

5.9 Searching of staff

Searching of staff suspected of committing a breach of security It is an offence for members of staff to permanently remove property belonging to the Trust without written authority. Failure to seek authority from line management could result in disciplinary action or criminal proceedings being taken.

If any member of staff is suspected of committing a breach of security through the possession of prohibited, controlled or stolen items they will be asked by their manager to consent to a search of their personal belongings, including lockers. Two members of staff as well as the individual concerned must be present at the time of the search. If the individual refuses to a search being undertaken the manager will consult with the HR department regarding the possibility of instigating disciplinary proceedings.

Reporting Crime & Subsequent Actions:

All crime including theft should be reported as a crime and the security team notified in the first instance, so that appropriate investigation of the theft may be organised and undertaken by the Security Team and/or local police. Trust equipment and assets considered to be ‘missing’, ‘borrowed’ or otherwise displaced must be subject of robust checks and investigation.

In the event that the equipment is not located a report of crime must be made via a Datix report and call to the police. The police crime number must be added to the Datix report along with any attending police officer's details (name & collar number).

Searching of staff

It may be necessary because of the circumstances of a theft, other crime or current investigation to ask personnel working or visiting on site to consent to a search of him/her and their outer clothing only, bags/cases and vehicle. The law on this subject is quite clear: no person has any right to search another without that person's consent having been freely given. Searching will only be undertaken as part of a current investigation. The Trust reserves the right to check and search lockers, desks, offices and property spaces. If required these can be forcibly opened and further details are contained in the Trust Locker Policy.

In all other cases the following procedure must be followed:

- The person is to be asked for consent to the search of their outer clothing or possessions and their work area, if that is provided by the Trust
- The person must be informed that she/he has the absolute right to refuse consent. No persuasion of any nature is to be made to obtain consent and no threats, implied or expressed
- If consent is refused, the proposed search will NOT take place. A refusal may initiate involvement by the police.
- If full and free consent is obtained, the person is to be asked to nominate a witness to be present. If he/she cannot nominate a witness, he/she is to be asked to approve a witness nominated by the searcher. No search must be carried out in the absence of a witness or in the presence of a witness unacceptable to the person being searched.
- Females, their possessions, lockers, office and outer clothing must only be searched in the presence of another female. In all cases a personal search must be confined in outer clothing: under no circumstances is a body or other intimate search to be made.
- Accurate notes must be made, and retained, in respect of the search and the subsequent sequence of events. Dates, times, places, names of those searched, witness etc. must all be recorded in the Manager's and/or Security Officer's notebook
- If articles alleged to have been stolen are found, the facts must be noted, and the matter referred to a higher authority for a decision as to whether or not the investigation will continue, or the police informed. A list of the articles found in the person's possession is to be given to that person as soon as possible after the search.
- If nothing of an incriminating nature is found, the person is to be issued with a certificate stating that he/she was searched at (time) on (date) in (place) in the presence of (witness) and he/she was not in possession of the allegedly stolen items. The certificate must be signed by the person performing the search.

- It is anticipated that the occasions when searching individuals is considered desirable will be rare and that, generally, a case serious enough to warrant such a search may be referred to the police.

5.10 Security of Personnel

Identification
Whilst on duty all Trust staff, irrespective of status and including temporary, bank and agency and contracted staff, must wear a Trust identity (ID) card, except in circumstances where it poses a risk to health and safety e.g. in operating theatres. It must be produced when requested by a senior manager or member of the security team/unit. Individuals must report any loss or damage of the ID card on Datix and abide by the reporting conditions accepted under signature. All cards must be returned on termination of employment. Applications for a Trust ID card should be made via the appropriate form available on the Trust Intranet site and signed by their Line Manager.

The card remains the property of the Trust and can be withdrawn should the circumstances dictate. I/D and Smartcards withdrawn from staff under suspension are to be retained by the line manager and made available on their return to work. Managers must inform the BFS Business Security Unit of the card status to allow it to be disabled and enabled as required.

Suspicious persons or visitors
Staff should stop suspicious visitors from entering a ward or department and asked who they are visiting or the location of an appointment. An initial polite challenge should be made in every case and circumstances in which staff are uncomfortable or concerned should be reported to their Line Manager or directly to the security team on 01924 316354. Staff should never put themselves at risk and if in any doubt should inform the security team.

Restricted areas of access
Enhanced security arrangements are in place for the following areas:

- Medium Secure Unit – Newton Lodge
- Low Secure Unit – Bretton Centre
- Newhaven
- Unity Centre
- Dales Unit
- Unit Ward 18 and 19, Priestley Unit
- Roof areas
- Pharmacy

All entrance and exit doors must be secured such that access is only possible through dedicated entrances, via a swipe card, manual keys and/or keypad.

5.11 Unauthorised photography and recording

Unauthorised photography, sound and/or video recording is strictly prohibited on the Trust site and persons found engaged in this activity will be requested cease

immediately and to delete any data obtained or retained. The security team will inform the police of all occurrences.
Authority for photography and/or recording must be requested from a Trust senior manager, senior nurse or the Corporate Communications Department.

5.12 Agile Working and Lone Workers

All reasonable steps must be taken to ensure the safety of employees who, in the carrying out of their job responsibilities, may be required to work alone. This will be achieved by the development of appropriate procedures and working practices and ensuring that staff have the appropriate skills and equipment to enable them to work safely and securely. For further reference see the Trust's Lone Worker Policy and Agile work policy.

5.13 Personal safety alarms

Personal attack alarms are installed in various locations throughout the trust. Different systems are used depending on the service provided. It is the responsibility of the individual member of staff to check how the alarms systems are operated and what the response will be in that particular setting.

Ward based staff are provided with personal attack alarms and must carry them at all times. Ward based staff are responsible to ensure that the personal attack alarm is functioning correctly and tested in the Personal Infrared Transmitter (PIT) test box. Staff should never enter the clinical areas without first checking their PIT alarm is functioning. Each member of staff is responsible for the safe custody and usage of safety equipment which have been issued to them. For more information please refer to the Pinpoint Procedure or local alarms response procedure or the appropriate personal alarm system procedure for their local building.

5.14 Surveillance systems/CCTV

All surveillance camera systems (CCTV and ANPR) are used for the general purpose of crime prevention and detection and public safety. It is not intended that the CCTV and ANPR systems should be used by official law enforcement bodies, such as police forces, the security services or HM Revenue and Customs when carrying out specialised and/or surveillance or operations, such use would require the authorisation of the Chief Police Officer.

This policy, and the CCTV Code of Practice (issued by the Information Commissioner) on which the use of our systems are based, is intended to assist South West Yorkshire Partnership NHS Foundation Trust (SWYPFT) operators and users of CCTV and ANPR systems to understand their legal obligations when using CCTV. It is also intended to reassure the public that a standard is in place that controls the use of CCTV systems on SWYPFT owned or occupied sites.

More information around the use and access to CCTV footage is available within the Trust Surveillance Systems Policy.

5.15 Service users Property

SWYPFT will not accept any responsibility or liability for service users' property of money brought into the health service premises unless it is declared and handed in for safe custody.

Each service must develop local procedures to provide safe custody for money and other personal belongings handed in by service users for safekeeping, in line with Trust Service users Property Policy. Further advice can be sought from the Security Adviser and finance department.

5.16 Staff Personal Property

The trust expect staff to protect their own personal property and money at all times, by locking it away and using secure lockers or secure drawers. Staff are advised **not to bring valuable personal property to work.**

Portable equipment and other items should be secured in lockable rooms or cupboards when not in use. Trust security policies must be adhered to at all times: make sure you are aware of them.

Any concerns must be reported to the Security Adviser as they are your first point of contact for security reports and concerns. Report all lost, stolen and missing assets as soon as possible.

5.17 ID Badges and Car Parking Permits

All staff are to wear their issued ID badges while on SWYPFT business. Lost or stolen ID badges must be reported to the line management and reported on Datix.

Visitors and contractors must report to the appropriate reception area and collect a visitors/contractor's badge to be identifiable on the health premises.

All staff parking on SWYPFT sites must display a trust parking permit as described in the On-Site traffic and Parking Policy. This is to support better management of our car parks and to allow the security team to ensure they can contact staff if necessary.

6. References and associated documents

- CQC Fundamental Standards - Regulation 15: Premises and equipment (15(1)(b): Secure. http://www.cqc.org.uk/guidance-providers/regulations-enforcement/regulation-15-premises-equipment#guidance
- *Health and Safety at Work etc., Act 1974*. London: The Stationery Office.

- Health & Safety Executive. *(*1999). *Management of Health and Safety at Work Regulations SI 1999/3242.* HSE Books. Available at: www.hse.gov.uk
- NHS Counter Fraud and Security Management Service. (2005). *Safe and Se(cure). How You Can Help the NHS Protect Itself* NHS CFSMS. Available at: www.cfsms.nhs.uk
- NHS Counter Fraud and Security Management Service. (2003). *A Professional Approach to Managing Security in the NHS*. NHS CFSMS. Available at: www.cfsms.nhs.uk
- NHS Counter Fraud and Security Management Service. (2002). *The Policy & Operational Responsibility for the Management of Security in the NHS Statutory Instrument 2002/3039*. Available at: www.cfsms.nhs.uk

7. Referenced Policies

- Incident Reporting and Management (including Serious Untoward Incidents)
- Investigating and analysing incidents, complaints and claims to learn from experience
- Medicines Code
- Lone worker Policy & Guidance

- Pinpoint Procedure
- Lockdown Policy
- Police Liaison Policy
- Violence and Aggression at Work Policy
- Management of Aggression and Violence Policy
- Health & Safety Risk Assessment Policy
- Supporting staff involved in traumatic or stressful adverse events (incorporating incidents, complaints, claims)
- Trust Wide Health & Safety Policy

Appendix A

Equality Impact Assessment template to be completed for all policies, procedures and strategies

Date of assessment: 1 September 2020

	Equality Impact Assessment Questions:	**Evidence based answers & actions:**

1	**Name of the document that you are Equality Impact Assessing**		**Safe & Secure Environment Policy**
2	**Describe the overall aim of your document and context?** **Who will benefit from this policy/procedure/strategy?**		**Safe and secure environments within the Trust are concerned with the provision of safeguards to protect the safety of those who visit or work within Trust premises and the protection of property belonging to service users, visitors, staff and the Trust.** **The overall aim of this policy is to balance the rights and responsibilities of people using its services with those of employees, with a clear approach to health & safety risk management. It also aims to support staff, by ensuring that working environments which are controlled by the Trust are as safe and pleasant to work in as possible.** **All staff, service users and visitors**
3	**Who is the overall lead for this assessment?**		**Security Team**
4	**Who else was involved in conducting this assessment?**		**Safety & Resilience TAG**
5	**Have you involved and consulted service users, carers, and staff in developing this policy/procedure/strategy?** **What did you find out and how have you used this information?**		**The Safety & Resilience TAG and respective sub groups were consulted during the original development of the Policy.** **It was identified that the Trust required clear and unambiguous security information that was easily accessible. This was taken into account when developing this policy.**
6	**What equality data have you used to inform this equality impact assessment?**		
8	**Taking into account the information gathered above, could this policy /procedure/strategy affect any of the following equality group unfavourably:**	**Yes/No**	**Evidence based answers & actions. Where negative impact has been identified please explain what action you will take to remove or mitigate this impact.**
8.1	**Race**	**No**	
8.2	**Disability**	**No**	
8.3	**Gender**	**No**	

8.4	**Age**	**No**	
8.5	**Sexual orientation**	**No**	
8.6	**Religion or belief**	**No**	
8.7	**Transgender**	**No**	
8.8	**Maternity & Pregnancy**	**No**	
8.9	**Marriage & civil partnerships**	**No**	
8.10	**Carers (Our Trust requirement)**	**No**	
9	**What monitoring arrangements are you implementing or already have in place to ensure that this policy/procedure/strategy**		**A standardised approach to policy, development, approval and dissemination with an equality impact assessment.**
9a	**Promotes equality of opportunity for people who share the above protected characteristics;**		**Yes, the safe and secure environment is none discriminative and applies to everyone.**
9b	**Eliminates discrimination, harassment and bullying for people who share the above protected characteristics;**		**Yes**
9c	**Promotes good relations between different equality groups;**		**Yes**
9d	**Public Sector Equality Duty – "Due Regard"**		**Yes**
10	**Have you developed an Action Plan arising from this assessment?**		**No**
11	**Assessment/Action Plan approved by**		
	(Director Lead)		**Sign: Date:** **Title:**
12	***Once approved, you must forward a copy of this Assessment/Action Plan to the partnerships team:*** **partnerships@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 B - 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?	YES	
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	

Appendix C

Contacting Security Services

In all Emergency situations the Police must be contacted first on: 999

Managers are responsible to escalate appropriate security contact details to their staff and to endure staff are aware of the local security arrangements. Community staff must agree local lone working procedures and police and other emergency contact procedures within their own departments.

Wakefield Area, Fieldhead

Security contact numbers:

Fieldhead: **07771345275**
Kendray: **07920535209**
Security mobile 1**: 07824122960**
Security Mobile 2: **07824122962**
Security Mobile 3: **07824122966**

Working Times:

08.00 to 18.00, Monday to Friday

Security is available at Fieldhead from 08.00 to 18.00, Monday to Friday. Security will attend community premises on request.

Out of hours Support:

Outside of the normal working hours for non emergencies the porters can be contacted for assistance on **01924 316335** or mobile number: **07876230467;**

or the Police for non-emergencies on **101**;

and for emergencies the Police should be contacted on **999.**

Community Premises Security Support (Trust Wide)

Active Response Security:

Active Response Security is currently supplying the Trust with key holding and alarm response service to out of hour's security incidents, between the hours of 7pm and 7am. This service will respond to out of hours non emergencies i.e. alarm activation, disturbances and trespassing, broken windows etc.

Active can be contacted on:

- Main control room- 01226 288886
- Secondary control room number- 07734953774
- Manager on call- 07702810008

Emergency calls for immediate support must be directed to the Police on **999.**

Dewsbury Hospital

Switchboard: **01924 541000**

Contact: Security on:

- **07748321348**

Calderdale Hospital

Contact Switchboard on:

- **01422 357 171** – switchboard are in radio contact with security 24 hours a day.

Staff are advised to test these number regularly as number can change.

Barnsley Area, Kendray

Out of hours support

Kendray: Bleep holder or alternatively, Active Security patrols via their control numbers listed as above.

LIFT Buildings: All under MITIE jurisdiction.

All Clinics. Key holding and response to fire and intruder alarms plus the securing of buildings is carried out by Active Response with advice when required given by on call engineer.

NB: Whenever staff are in an emergency situation or if there is an immediate danger to a person, the police should be contacted via 999 and asked to attend immediately.

d

Appendix D - Version Control Sheet

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

Version	Date	Author	Status	Comment / changes
1.1	11th September 2008	Roland Webb	Draft	Updated and revised policy in line with NHSLA requirements
1.2	22nd September 2008	Roland Webb	Draft	Updated and revised policy in line with comments from consultation process.
1.3	23rd September 2008	Roland Webb	Draft	Further development following comments from Gemma Hannon, Portfolio Manager – Compliance Clinical Governance Support Team
1.4	24th September 2008	Roland Webb	Draft	Additional comments and suggestions received from the consultation process
1.5	25th September 2008	Roland Webb	Draft	Insertion of additional “Risk Assessment”, “Monitoring” & “Action Planning” information.
1.6	1st October 2008	Roland Webb	Draft	Final draft agreed after meeting with Alan Davis, Julie Eskins, Stuart Andrews & Roland to satisfy policy meets organisational needs as well as NHSLA criteria.
1.7	14th October 2008	Roland Webb	Draft	Revised policy detailing clearer process (3.4) of risk assessment process & how this is communicated, ultimately to board level and adding significant risks to Service Delivery Group Risk Registers (5.9)
1.8	November 2008	Roland Webb	Draft – Final version	Approval at EMT
2.1	21 May 2010	Johan Celliers	Review	Revision of Policy for NHSLA Secure Environments compliance to include reference to Trust Lockdown guidance (7.7). Also new references to access control (7.8), SMS Alerts (7.9), lone workers (7.10), patient property (7.11), ID badges (7.12) and revision of Trust wide security contact details (7.1).
2.2	June 2010	Johan Celliers	Review	Consultation with Clinical Governance Support Team re compliance requirements to include timescales for producing Risk Profile (See Trust Lockdown Policy Appendix F, G, H) for all Trust premises as included.
2.3	July 2010	Johan Celliers	Review	Included from Linda Hollingworth and minor alteration after meeting NHSLA assessor.
2.4	13 August 2010	Johan Celliers	Review	Discussed and reviewed with Julie Eskins in line with NHSLA requirements
2.5	28 September 2012	Johan Celliers	Review	Consultation with Barnsley BDU Estates and Facilities Department regarding Security provision.
2.6	12 November 2012	Johan Celliers/Helen Roberts/Gemma Hannon/Roland Webb	Minor update	Update includes hyperlinks not originally available & clarifies role of Health & Safety TAG/Sub-groups in developing action plans
2.7	9 February 2016	Johan Celliers	Minor Update	Minor updates to various areas but main change relates to new contact details for newly appointed security contractor.
2.8	21 February 2016	Johan Celliers	Update in line to	Minor updates as per various colleagues re pharmacy, Hs and EP TAG, and appendices.

			requested comments	
2.9	January 2018	Johan Celliers	Scheduled Review	
3.0	August 2020	Johan Celliers	Scheduled review	Updates to roles and responsibilities and Section 5: Local Security Information to support Safe and Secure Environments