# Physical Security Management Policy

***Please be aware that this printed version of the Policy may NOT be the latest version. Staff are reminded that they should always refer to the Intranet for the latest version.***

| | |
|---|---|
| **Purpose of Agreement** | The purpose of this policy is to ensure the safety and security of personnel, patients, visitors, volunteers and contractors and to protect NHS property premises and valuable assets against theft and damage, to produce a safe environment in which to deliver uninterrupted quality healthcare. |
| **Document Type** | X Policy ☐ SOP ☐ Guideline |
| **Reference Number** | Solent NHS Trust/Policy/RK05 |
| **Version** | 3 |
| **Name of Approving Committees/Groups** | Policy Steering Group, Clinical Executive Group |
| **Operational Date** | February 2021 |
| **Document Review Date** | February 2024 |
| **Document Sponsor (Name & Job Title)** | Chief Nurse |
| **Document Manager (Name & Job Title)** | Accredited Security Management Specialist (ASMS) |
| **Document developed in consultation with** | H&S Sub Committee |
| **Intranet Location** | Business Zone > Policies, SOPs and Clinical Guidelines |
| **Website Location** | Publication Scheme |
| **Keywords (for website/intranet uploading)** | Security, Violence, Theft, Vandalism, Crime, Damage, ASMS, NHSLA, Policy, RK05 |

**Review Log**
Include details of when the document was last reviewed:

| Version Number | Review Date | Name of reviewer | Ratification Process | Reason for amendments |
|---|---|---|---|---|
| v1 | Dec 2016 | GE | | Initial Issue |
| v2 | April 2020 | Stuart Francis | Approved as part of the Covid-19 review of policies | Amends made to policy content to bring up to date, insertion of overarching Emergency Statement and expiry extended to March 2021 |
| v3 | January 2021 | Stuart Francis | Policy Steering Group, Clinical Executive Group | |

**Amendments Summary**

| Amend No | Issued | Page(s) | Subject | Action Date |
|---|---|---|---|---|
| 1 | Nov 2016 | | Physical Security Policy Re-written | Nov 2016 |
| 2 | April 2020 | | As per above | April 2020 |
| 3 | January 2021 | No material amends | Added ref. to Violence Prevention and Reduction Standard and minor typographical changes as suggested by LCFS. | January 2021 |


**Executive Summary**

This policy gives comprehensive guidance to ensure staff & management are aware of the procedures to follow around physical security in place within the Trust,

The policy will reflect the standards when it comes to physical security measures employed by the Trust to ensure the safety and security of staff and patients utilising Solent NHS Trust facilities.

**CONTENTS**

Staff are expected to adhere to the processes and procedures detailed within this policy. During times of national or 'Gold command' emergency Solent NHS Trust may seek to suspend elements of this policy in order to appropriately respond to a critical situation and enable staff to continue to work in a way that protects patient and staff safety. In such cases Quality Impact assessments will be completed for process changes being put in place across the organisation. The QIA will require sign off by the Solent NHS Ethics Panel, which is convened at such times, and is chaired by either the Chief Nurse or Chief Medical Officer. Once approved at Ethics panel, these changes will be logged and the names/numbers of policies affected will be noted in the Trust wide risk associated with emergency situations. This sign off should include a start date for amendments and a review date or step down date when normal policy and procedures will resume.

## 1. INTRODUCTION & PURPOSE

### 1.1 Introduction

1.1.1 The below policy is designed to support employees by raising awareness of security related Policies, Processes and Procedures within the Trust that may affect the safety and security of employees, patients and visitors. The policy supports a pro security culture where the protection of trust infrastructure such as critical, vulnerable and valuable assets is the responsibility of all. This policy supports the aims of Solent NHS Trust in the delivery of high quality clinical care services.

1.1.2 The core of this Policy is guided by the NHS Standards for Providers and the NHS Condition 24 Violence and Aggression Standard and the NHS standard contract which is considered as best practise.

### 1.2 Purpose

1.2.1 As part of our commitment to ensure the delivery of a high quality and safe working environment for our staff, patients and visitors who access our facilities, we will;

(A) Recognise and accept obligations relating to the management of security as far as are reasonably practicable.

(B) Ensure the security of people and property within Solent NHS Trust is a concern of ALL of its employees, contractors and volunteers.

(C) Solent NHS Trust will ensure that all possible measures are taken to deliver a secure environment for all who work or receive treatment.

1.2.2 Accountability for security of the trust lies with the Chief Executive Officer who works closely with the Deputy Chief Executive Officer who holds the position of Security Management Director (SMD), the organisational structure supports responsibility for delivering a secure environment at all levels.

1.2.3 Solent NHS Trust provides for the day to day management of security through the post of Accredited Security Management Specialist (ASMS), who consults the various managers on operational security issues to the in-house team of security personnel operated by the various Facilities Departments and Service leads.

1.2.4 The guiding principles are to seek to achieve a secure environment that protects patients, staff and visitors and their property as well as the physical assets of the organisation

1.2.5 The SMS is the security arm of the Trust with fraud matters being dealt with by the Trusts LCFS (Local Counter Fraud Specialist). This LCFS role is outsourced and will be provided as per the Local Fraud, Bribery and Corruption Policy. Both ASMS and LCFS will work together where necessary to reduce Fraud, Bribery and corruption within the Solent NHS Trust.

1.2.6 Incidents of crime and breaches of security that are particularly sensitive where employees have been victims of crime and affected will be provided with support and their wishes around reporting of criminal offences will be respected as much as is reasonably practicable.

1.2.7 The organisation believes that effective security is an integral part of all operational activity. The responsibility for compliance with this policy is delegated to all directors, managers and staff to an extent consistent with their position. Security is everyone's business.

## 2. SCOPE & DEFINITIONS

2.1 This policy applies to all locum, permanent and fixed term contract employees (including apprentices) who hold a contract of employment or engagement with the Trust, and secondees (including students), bank, volunteers (including Associate Hospital Managers), Non-Executive Directors, and those undertaking research working within Solent NHS Trust, in line with Solent NHS Trust's Equality, Diversity and Human Rights Policy. It also applies to external contractors, Agency workers, and other workers who are assigned to Solent NHS Trust.

## 3. PROCESS/REQUIREMENTS

### 3.1 MANAGING VIOLENT INCIDENTS AND VERBAL ABUSE BY SERVICE USERS AND MEMBERS OF THE PUBLIC

3.1.1 All line managers and departmental heads need to ensure that they refer to the Management of Violence, Aggression Policy when preparing local procedures for protecting staff from violence and aggression and for ensuring the correct actions are undertaken in the event of an incident. All staff is trained to the appropriate level for their appointment in accordance with the Learning & Development training needs analysis.

### 3.2 PHYSICAL SECURITY

3.2.1 All services provided by Solent NHS Trust must incorporate good security working practices into their operating procedures, together with security design as part of an overall strategy.

3.2.2 Solent NHS Trust will have systems in place to ensure an appropriate response to incidents including:

- Recording all incidents on a dedicated security database (Ulysses), whereby trends can be identified and risks assessed.

- Audit Safeguard Reports indicating trends and the needs for action to be taken in compliance with all relevant security policies via quarterly reports submitted to the Health & Safety Sub Committee.

### 3.2.3 **Security of Departments**

Where suitable all departments Must be fully secured when they not in use either during the day or Out of hours. It is best practice for departments to:

- Create and Maintain where possible Key Management systems whether they are physical key management systems or they are an interim / temporary procedure
- Use a risk based approach to allow only authorised personnel (lists of authorised persons should be kept with key cabinets), who must complete the key register and sign their entry, should they remove keys from the appropriate storage facility.
- Records will be auditable in cases where an investigation is subsequently required.

### 3.2.4 **Security of Personal Property**

It is the responsibility of each member of staff to secure their own property against loss or theft. Where possible all personal property should be locked away. The Trust accepts no responsibility for personal possessions lost or damaged on its property.

Staff should use lockers, drawers, cabinets where provided, in staff rooms and/or changing rooms to secure their property. Personal property should be identifiable. Handbags, purses and wallets must not be left lying about or in coat pockets; they should be deposited in a secure place or kept on your person or within eyesight of the owner at all times.

### 3.2.5 **Security of Patient's Property**

Departments must have in place local procedures to protect patients/clients cash and valuables. The procedures must take into account all aspects of the security of staff handling valuables and cash.

On admission, patient's property should be checked; an inventory made of valuables and noted; a disclaimer form to be signed by the patient and Staff member; a receipt issued and items deposited in a secure location with restricted access.

Property should not be given to relatives without patients consent.
The Trust cannot be held responsible for any valuable property or cash not handed in for safe keeping.

Patients are to be encouraged not to bring valuables or large sums of money onto any Trust premises.

If a patient is unable to sign a disclaimer on admission for whatever reason, two members of staff should be present when property is taken from the patient and a written and signed explanation entered onto the disclaimer form.

The Trust recognises the importance of providing patients/clients with a secure method of keeping personal items when they are admitted to Trust inpatient facilities.

3.2.6 **Protection of NHS Property and Assets**

All ward and department managers are to ensure they provide information to the Trusts Property Systems Officers regarding non clinical assets to allow MiCAD to be kept up to date. All clinical assets must be listed on the Medical Devices Asset Register; this is managed by the Health & Safety Manager.

All valuables or "attractive" items are to be kept in locked containers/rooms when not in use. Most thefts that occur are opportunist by nature and by taking simple precautions will reduce financial loss to the Trust and patients ensuring a more effective service.

It is strongly recommended that items are logged in and out of the secure room/container and recipients are made to sign for the item. This will prevent items being reported stolen when they have been legitimately handed to another staff member.

3.2.7 **Identification – Official Visitors and Contractors**

Due to the high incidence of petty theft and distraction burglaries at NHS sites across the country, contractors and other personnel, who visit a site/department for business purposes, must be issued with a visitor's identification badge that must be displayed at all times when personnel are on the premises. This will be signed for in the register held at the appropriate reception area. The member of staff who is responsible for the contractor will then arrange for the visitor to be escorted to the relevant department.

All units where there is high level of mental health care, contractors must read and sign site rules for the safety of clients and themselves.

On leaving, the visitor's badge must be returned. All relevant times should be recorded in the register held within the department. Unreturned badges are to be reported to the Security Staff/Site Manager/Kier, who should contact the firm/visitor and arrange for its return.

3.2.8 **Staff Identification**

This policy requires that all staff wear identification badges. Photographic identification badges for staff will be produced in accordance with the ID Badge system. Staff members are to ensure their badges are visible at all times while at work or one Solent premises.

**3.2.9 Challenging persons not displaying a Trust ID Badge**

Any person who is not wearing a visible ID badge whom is found in any non-public area must be challenged. A polite but assertive challenge should be all that is required for that person to identify themselves, such as, 'Can I help you?' Suspicious behaviour should be reported to your site/senior manager and/or security staff or the ASMS where present as well as on the Ulysses Reporting System.

3.2.10 **Security Surveillance Systems**

The installation of Security Surveillance Systems at sites identified as benefiting from the facility is for the primary purpose of deterring and detection of criminal activity against the organisation, its staff or visitors. Please refer to the Security Surveillance Policy.

Where crime is committed any relevant data captured by surveillance cameras may be used as evidence to support criminal or civil prosecution of the perpetrator(s).

Whilst crime within NHS premises in most instances is perpetrated by outside individuals, there are rare occasions, when crimes are committed by members of staff. Whilst the NHS routinely installs overt systems to deter crime, it is considered essential that occasionally it may be beneficial not just to deter but, in selected instances, to catch offenders in the act so that more appropriate action can then be taken. Accordingly, the use of covert surveillance cameras in selected situations may be undertaken. To regulate the use of covert filming authorisation must be firstly obtained from The Chief Executive Officer of the trust then permission obtained from the Police through the Chief Officer in accordance with the Regulation of Investigatory Powers Act (RIPA) 2000. **The only method of obtaining this authority is through the ASMS and the SMD who will contact the above for permission.**

**Please refer to the Trust CCTV Policy**

## 3.3 SECURITY INCIDENTS & REPORTING PROCESS

3.3.1 Solent NHS Trust expects that staff, patients and visitors will behave in a manner that respects others, NHS premises and assets. The organisation will not tolerate any form of criminality or wanton disregard for the integrity of its staff, patients, premises and assets or anti – social behaviour.

3.3.2 **Sanctions against perpetrators**

A range of measures can be taken by NHS Trusts depending on the nature and severity of an incident which may assist in the management of unacceptable behaviour by seeking to reduce the risks and demonstrate acceptable standards of behaviour, these may include:

- Verbal warnings
- Acceptable Behavioural Agreement (letter to patient) (ABA);
- Written warnings (letter to patient setting out plan of communication)
- Exclusion from attending Trust Premises (119 and 120 CJIA Act)
- Civil Injunctions / Prosecutions (Person 2 Person) (Proceeds of Crime) as well as Criminal Behaviour Orders (CBO's)
- Restorative Justice Resolutions or Disposals (RJR, RJD)

Whilst a verbal warning would precede any Acknowledgement of Responsibilities Agreement and this would precede the Withholding of Treatment, there is no requirement to escalate the response in any particular order if the situation warrants immediate action.

A Verbal Warning or Acknowledgement of Responsibilities Agreement may not be appropriate or possible if the perpetrator is not aware or considered responsible for their actions.

In all instances, regardless of whether or not the Police decide to prosecute, the ASMS, in consultation with the Trusts legal team, will decide whether preventative action, if any, should be taken to reduce further or related future incidents.

Where it is decided that there is a need to exclude an individual from attending trust premises, a full investigation must be carried out prior to the issue of an exclusion letter. This is to ensure that the full consideration is made of any legitimate need to attend the site. The SMD must agree to this course of action.

Furthermore an exclusion letter may only be issued on behalf of the Trust by the ASMS, once it has been vetted by the Trusts legal team. Any exclusion letters issued, must contain a review date no later than 12 months after the issue date and information on appealing the exclusion order. Details of this procedure can be found in the Prevention, Management of Violence & Aggression Policy.

3.3.3 **Reporting Process**

On receipt of a verbal report of any of the prohibited behaviours above, individuals/managers are to raise a report on the Online Risk Management System (incident reporting system) The ASMS may be contacted by telephone for support and will provide advice and guidance on appropriate measures in accordance with this policy.

3.3.4 **Partnership Organisations and Associated Disciplines**

**Hampshire & Isle of Wight Counter Fraud Service (CFS)**

The Counter Fraud Service supports Solent NHS Trust as a specialist organisation with the commitment to protect the NHS by ensuring that resources made available to patient care and services are not lost to fraud & corruption.

The Chief Finance Officer works with the Local Counter Fraud Specialist to prevent and detect fraudulent activities. Where suspected then an investigation will ensue and criminal proceedings and or disciplinary procedures may be implemented. See also the Freedom to Speak Up: Raising Concerns Policy.

**Information Security**

Refer to:

Information Governance Policy
Data Protection Act
Access to Records Policy
Freedom of Information and Environment Information Regulation

**Police Counter Terrorism Security Advisers (CTSAs)**

Whilst there is no evidence to suggest that the NHS is more at risk from terrorism than other public service organisations, staff should maintain a level of alertness commensurate with the current national threat.

Advice and guidance on what to do in the event of the discovery of a suspicious package or postal/telephone threat are contained in Policy for Suspect Packages

### 3.4 RISK ASSESSMENTS

#### 3.4.1 Risk Assessment Process

It is the responsibility of the ASMS to conduct site and department security risk assessments in conjunction with Service managers / Premises managers for each site, building, ward and department within the Trust. Where it is thought necessary, the Manager will contact the ASMS who will arrange for this assessment to be undertaken.

Crime Reduction surveys should be undertaken by the ASMS.

Risk assessments should be undertaken to ensure the:

- Physical security of the ward/ department
- Physical security of the assets in the ward /department
- Personal safety of staff, patients and visitors in the ward/department
- Personal safety of staff based in the ward or department, but working outside the premises.

Managers of community based services are to ensure that full risk assessments are conducted for all staff ensuring that full reference is made to the organisation's Lone Working Policy where appropriate.

The risk assessment will be used to identify the physical or management controls necessary to reduce or eliminate the risks, and to develop proposals for improved security across the Trust to protect staff, patients and visitors, and the assets of the Trust. This will be co-ordinated by the ASMS.

Where there are significant weaknesses identified that it is difficult to rectify an entry must be made in the individual Service Line Risk Register in accordance with Solent Clinical Risk Assessment and Management Policy if appropriate.

3.4.2 Copies of all site, building, department and ward security risk assessments are to be forwarded to the ASMS.

## 4. ROLES & RESPONSIBILITIES

### 4.1 The Chief Executive

The Chief Executive is accountable for the overall safety and security of the entire Trust and ensuring that the Trust complies with current security directions, legislation for all matters of security.
The Chief Executive will nominate a board level director (**Security Management Director**) who will be accountable to the Chief Executive for all aspects of security matters.

### 4.2 Deputy Chief Executive Officer/ Chief Finance Director (Security Management Director SMD)

4.2.1 The Trust Deputy Chief Executive Officer (SMD) will be nominated to take overall operational responsibility for all aspects of Security Management within the trust. The SMD will work

closely with the ASMS who will conduct much of the proactive and reactive work towards dealing with incidents of violence against staff, ensuring the following are considered:

### 4.3 Accredited Security Management Specialist (ASMS)

4.3.1 The nominated Accredited Security Management Specialists (ASMS) are accredited consultants who provide professional skills and expertise to tackle security management issues across a generic range of proactive and reactive action. The overall objective of the ASMS will be to work on behalf of Solent NHS Trust to deliver an environment that is safe and secure so that the highest standards of clinical care are provided to patients.

4.3.2 The ASMS will:

- Have passed the accredited training from NHS security management service.
- Be responsible for the Security of all the locations within Solent NHS Trust: carry out reviews, inspections, reports and advise the board through the SMD on all matters of security provision.
- Work closely with any ASMS or any LSMS from other trusts, to respond to all Security Management initiatives and security alerts.
- Provide advice to managers at all levels on security measures in how to deal with violence and aggression or challenging behaviour.
- Provide assistance to managers implementing risk reduction measures and post-incident management.
- Monitor the effectiveness of implementation of the security policy by means of Security Surveys/Risk Assessments.
- Report results of Security Surveys/Risk Assessments undertaken to the Health & Safety Committee and provide assurance of any actions required and completed.
- Ensure there is a prompt review with service leads of any significant violent incident and that it is used to evaluate policy guidelines and recommend security safety systems to avoid further incidents i.e. Access Control, Panic Alarms and Surveillance Cameras.
- Work with the Service Line Managers, Directors to improve all aspects of Security within Solent NHS Trust
- Provide assistance to managers undertaking violence at work risk assessments and report to the Health & Safety Committee on the implementation of risk assessments by service line.
- To Submit quarterly reports to the Health & Safety Committee as well as an annual security report and Self Review Tool (SRT) to the SMD.
- To be licensed with PSL Public Space Licence to ensure that where necessary CCTV footage can be viewed and gathered in case of any evidential need.

### 4.4 Associate Director of Estates and Facilities

4.4.1 The Associate Director of Estates and Facilities has the responsibility for premises development, including the physical security of premises. As such they need to work in partnership with the ASMS to cover all aspects of security at the design stage of any new premises or when major refurbishments take place, as required by a range of Heath Building Notes.

**4.5 Other Associate Directors (ADs)/Operational Directors/Clinical Leads**

4.5.1 It is the responsibility of all ADs/Operational Directors and Clinical Leads to:

- Disseminate the Security Policy within the area of their responsibility
- Ensure the implementation of the Security Policy within the area of their responsibility by providing support and advice to their managers
- Co-ordinate security issues with all staff, whether employed directly or indirectly.

4.6 **Health & Safety Manager**

4.6.1 The Health & Safety Manager is responsible for working with the ASMS to ensure that Health & Safety aspects of any security incidents are dealt with in the appropriate manner. The H&S manager will work with the ASMS to ensure that all security practices and procedures correspond to Health & Safety legislation.

4.7 **Service Line Managers / Premises Managers**

4.7.1 The Service Line managers / Premises Manager are responsible for matters relating to security, violence prevention and personal safety within their own areas, and will ensure the operational implementation of the Security Policy.

4.7.2 They will:

- Seek advice and support when security related incidents or breaches occur within their areas or departments
- Work with the ASMS to improve all aspects of security within their own areas by supporting, where practicable, all security improvements recommended by the ASMS
- Work with the ASMS to ensure that security surveys for all Solent NHS Trust premises are carried out, recorded and appropriately acted upon
- Liaise with managers and departmental heads in matters of security as appropriate
- Escalate concerns to their line managers and ASMS
- Work with the ASMS to conduct site and departmental security risk assessments for each site, building, ward and department within the Trust. Where it is thought necessary, the manager will request the ASMS to arrange this assessment to be undertaken.

**4.8 Managers and Departmental Heads' Responsibilities**

4.8.1 Managers and Departmental Heads in the event of any security breach, security incident or criminal activity, must ensure that

- Any departmental specific risk assessment process is completed.
- Any incident is recorded on the trust incident management system (Ulysses)
- The ASMS is notified of any security breaches, incidents or criminal activity for advice to be sought.
- They work with the ASMS to complete a Crime Reduction Survey report with all the relevant findings and recommendations.

4.8.2 Managers and departmental heads should implement a procedure to record details of all valuable or critical or clinical items within their areas or departments i.e. Make, Model, Part or Serial Numbers any identifiable features or Marks etc.

4.8.3 They should also:

- Ensure that arrangements are made to secure the Department out of working hours together with the safe custody of keys.

- Ensure, or delegate the responsibility of setting of any security alarm or device to protect the property out of hours.

- Ensure records are kept of all keys issued to staff in their Department/Directorate and reporting all losses of keys to their Service Managers.

- Seek advice from the ASMS to ensure that the highest standard of security is maintained within their Department/Directorate.

- Ensure all staff employed by the Solent NHS Trust, including Bank and Agency staff, Contractors and Official Visitors wear an ID badge at all times.

- Ensure that all staff members are made aware of this Physical Security Management Policy and fully understand its content and their responsibilities.

4.8.4 Managers and heads need to assess the impact on security of new projects and changes.

**4.9 The Operational Security Team (Guards)**

4.9.1 The security teams are a support service providing 24 HR security of the site at St James' Hospital (SJH), St Mary's Hospital Campus (SMHC) and Western Community Hospital (WCH) and will be managed by the relevant premises manager for that site.

4.9.2 Additionally, the guards are there to:

- Ensure that they are adequately licensed with SIA Security Industry Authority Licence (SIA)

- Be trained in the use of the installed Surveillance Camera systems on their sites and where necessary be (PSL) Public Space Licence certificated.

- Operate surveillance cameras and review following incident in accordance with the Surveillance Camera Policy

- Retrieve and prepare footage as required to provide evidence from Trust CCTV systems as per their training and Trust CCTV policy.

- Maintain a physical security presence of the site on a day to day basis as guided by the Premises manager.

- Maintain security infrastructure and systems such as fire/intruder alarms response, lighting etc.

- Patrolling of premises, providing a reassuring presence of security

- Support staff who request assistance relating to any incident or breach

- Support the ASMS in any investigations as directed by the Head of Facilities

- Support clinical staff to maintain staff retreat procedures should this be required in clinical areas.

4.9.3 Where the use of private security companies are considered to provide guards and/or surveillance camera monitoring services, The ASMS should be consulted prior to the signing of any contracts. The security company contract manager is to provide a full copy of the company assignment instructions for that site to the ASMS immediately upon commencement of the contract.

4.9.4 Any Resilience contract must be agreed with the ASMS before signing off or any commencement of the contract occurs. The ASMS must be provided with any assignment instructions required for the duration of the contract.

**4.10 Responsibilities of the Employee**

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

4.10.2 Staff should be aware of their responsibilities in protecting at all times, the assets/property of patients, visitors and the organisation. Where specific security procedures exist, staff must abide by them at all times. Where staff know or suspect a breach in security, they must report it immediately via the Online Risk Management System and at the earliest opportunity to their line manager, ASMS or their Clinical Manager.

4.10.3 All staff is reminded that it is an offence to remove property belonging to the organisation without written authority. Failure to seek authority from their line manager could result in disciplinary action or criminal proceedings being taken.

4.10.4 Staff members are responsible at all times, for the protection and safe keeping of their private property.

4.10.5 The ASMS will, if requested, advise staff on the security of their property. Any loss of private property must be reported without delay. If private property has been stolen, then it is the owner's responsibility, not Solent NHS Trust's responsibility to contact the Police.

4.10.6 Solent NHS Trust will not accept liability for the loss of, or damage to private property including motor vehicles or other modes of transport. Motor vehicles are brought onto the sites entirely at the owner's risk.

4.10.7 All employees including contractors must wear their ID Badges in a visible manner at all times regardless of standing within the Trust. However this is not an acceptable reason not to wear ID. Both staff and patients need to be assured that the person treating them or visiting that area is genuine. ID Badges are provided to all staff on induction. Lost, mislaid or badge changes must be reported via the Online Risk Management System and to the Security team at SMHC. Any staff requesting a new or replacement ID card **MUST** complete the appropriate HR form and provide appropriate ID e.g. copy of their contract or passport. On leaving the Trust ID badges must be handed into the team leader/ senior manager for that area, who should locally destroy the card immediately. Any access control cards/fobs must be returned to the premises manager for the area that it was issued to enable its deletion from the system.

4.10.8 All employees must recognise the responsibility they have for the confidentiality of the information they hold and use, in particular patient information. They must comply with all local departmental procedures and protocols that ensure the security of that information and prevent it being compromised in accordance with the Trusts Information Governance Policy.

4.10.8 Employees have a responsibility to ensure that they report all incidents in a timely manner and ensure that they use the Trust Incident management system (Ulysses) they must:

- Report incidents to line management / ASMS as soon as practicable. And place them on the Trust Incident Management system, if not possible then to ensure it is completed within 24 hours.
- Be aware of this policy and the trust Incident Reporting Policy.
- Consider and, when appropriate, implement the Solent NHS Trust 'Being Open' Policy.
- Give details of the incident and any identified actions on the incident reporting form.
- Report any risks that could warrant further investigation.
- Be fully open and co-operative with any reporting and investigation process but also the Solent NHS Trust HR Investigation Policy and Counter Fraud Policy.

### 4.11 Estates and Service Project Development Teams

4.11.1 Project Managers for site & building development/refurbishment projects are to ensure that the ASMS is consulted regarding proposed security systems and all security measures at all Trust occupied locations.

### 4.12 TRUST OVERALL - RECOVERY OF FINANCIAL LOSSES FOLLOWING THEFT/CRIMINAL DAMAGE

4.12.1 Solent NHS Trust will seek to recover all replacement/repair costs and associated administrative costs from persons who are identified as being responsible for acts resulting in the loss of or damage to NHS property or assets.

## 5. TRAINING

5.1 Solent NHS Trust recognises the need for effective training of staff to deal with security related issues and will ensure security training is provided by the ASMS with regard to:

- Conflict Resolution Training and ASMS Awareness to reduce the likelihood of assault

Training will be provided by the PMVA Lead for the trust with regard to:

- Prevention & Management of Violence and Aggression
- Breakaway Techniques.

5.1.1 The Security team are to possess Personal Security Industry Authority (SIA) Licences relevant to any Manned Security Guarding that takes place on Solent Sites. Any licence specific to a skill set must also be possessed (Public Space Licence PSL for monitoring CCTV). Operational Supervisors must hold full SIA licences such as DS licences,

## 6. EQUALITY & DIVERSITY AND MENTAL CAPACITY ACT

6.1 Please see Annex A For the updated Equality & Diversity and Mental Capacity Act Impact Assessment (IA).

## 7. SUCCESS CRITERIA / MONITORING THE COMPLIANCE OF THIS POLICY

7.1 The ASMS will conduct the Trust Self Review annually. The ASMS will also produce a Quarterly Report and present this for review at the Health and Safety Sub Committee meeting.

7.2 The ASMS, through the SMD is to present an annual report to the Board of Solent NHS Trust highlighting the year's activities and achievements and identifying challenges for the coming year.

## 8. REVIEW

8.1 This document may be reviewed at any time at the request of either staff side or management, but will automatically be reviewed 3 years from initial approval and thereafter on a triennial basis unless organisational changes, legislation, guidance or non-compliance prompt an earlier review.

## 9. REFERENCES AND LINKS TO OTHER DOCUMENTS

Health and Safety at Work Act 1974. London: The Stationary Office.

## 10. ASSOCIATED TRUST POLICIES

Suspect Package Policy
Risk Management Policy
Emergency Planning Policy
Adverse Event Reporting Policy
Health & Safety Policy
Lockdown Policy
Lone Working Policy
Management of Violence and Aggression Policy
Local Fraud, Bribery & Corruption Policy
Freedom to Speak Up: Raising Concerns Policy

## 11. GLOSSARY

| | |
|---|---|
| CCTV | Closed Circuit Television |
| AC | Assurance Committee |
| ASMS | Accredited Security Management Specialist, |
| SMD | Security Management Director |
| LCFS | Local Counter Fraud Specialist |
| ASMS | Accredited Security Management Specialist |
| Criminal Damage | Damage caused by any person to the property of another without Lawful consent can include negligent acts. Does include graffiti and vandalism |
| Physical Assault | The intentional application of force to the person, without lawful justification resulting in physical injury or personal discomfort. |
| Clinical Assault | The application of force to the person, without lawful justification, due to the clinical condition, resulting in physical injury or personal discomfort. |
| Non-Physical Assault | The use of inappropriate words or behaviour causing distress and or constituting harassment. |
| Skyguard / App | Mobile phone based monitored personal attack system for Solent NHS Lone workers to summon assistance. Provided in Device or App format |
| Micad | Trust Molecular Imaging Contrast Agent Database |

## Equality Analysis and Equality Impact Assessment

**Equality Analysis** is a way of considering the potential impact on different groups protected from discrimination by the Equality Act 2010. It is a legal requirement that places a duty on public sector organisations (The Public Sector Equality Duty) to integrate consideration of Equality, Diversity and Inclusion into their day-to-day business. The Equality Duty has 3 aims, it requires public bodies to have due regard to the need to:

- **eliminate unlawful discrimination**, harassment, victimisation and other conduct prohibited by the Equality Act of 2010;
- **advance equality of opportunity** between people who share a protected characteristic and people who do not;
- **foster good relations** between people who share a protected characteristic and people who do not.

**Equality Impact Assessment** (EIA) is a tool for examining the main functions and policies of an organisation to see whether they have the potential to affect people differently. Their purpose is to identify and address existing or potential inequalities, resulting from policy and practice development. Ideally, EIAs should cover all the strands of diversity and Inclusion. It will help us better understand its functions and the way decisions are made by:

- **considering the current situation**
- **deciding the aims and intended outcomes of a function or policy**
- **considering what evidence there is to support the decision and identifying any gaps**
- **ensuring it is an informed decision**

## Equality Impact Assessment (EIA)

| Step 1: Scoping and Identifying the Aims | | |
|---|---|---|
| Service Line / Department | Security Management / Compliance | |
| Title of Change: | N/A | |
| What are you completing this EIA for? (Please select): | Policy | *(If other please specify here)* |
| What are the main aims / objectives of the changes | To update the current EIA to the new | |

Step 2: Assessing the Impact

Please use the drop-down feature to detail any positive or negative impacts of this document /policy on patients in the drop-down box below. If there is no impact, please select "not applicable":

| Protected Characteristic | Positive Impact(s) | Negative Impact(s) | Not applicable | Action to address negative impact: *(e.g. adjustment to the policy)* |
|---|---|---|---|---|
| Sex | | | ✓ | |
| Gender reassignment | | | ✓ | |
| Disability | ✓ | | | There may be some impact on people with disabilities, but it will be positive by the fact that anyone expressing concern over disability can have a Personalised Security Plan for their concerns to be considered. |
| Age | | | ✓ | |
| Sexual Orientation | | | ✓ | |
| Pregnancy and maternity | | | ✓ | |
| Marriage and civil partnership | | | ✓ | |

| | | | | |
|---|---|---|---|---|
| Religion or belief | | | ✓ | |
| Race | | | ✓ | |

*If you answer yes to any of the following, you MUST complete the evidence column explaining what information you have considered which has led you to reach this decision.*

| Assessment Questions | Yes / No | Please document evidence / any mitigations |
|---|---|---|
| In consideration of your document development, did you consult with others, for example, external organisations, service users, carers or other voluntary sector groups?) | Yes | Health and Safety Manager |
| Have you taken into consideration any regulations, professional standards? | Yes | NHS Standards for Providers<br><br>ICO Guidelines<br><br>NHS standard contract (condition 24) |

| Step 3: Review, Risk and Action Plans | | | |
|---|---|---|---|
| How would you rate the overall level of impact / risk to the organisation if no action taken? | Low | Medium | High |
| | ■ | ☐ | ☐ |
| What action needs to be taken to reduce or eliminate the negative impact? | As above there is no negative impact | | |
| Who will be responsible for monitoring and regular review of the document / policy? | The ASMS and Health and Safety Manager | | |

| Step 4: Authorisation and sign off |
|---|

*I am satisfied that all available evidence has been accurately assessed for any potential impact on patients and groups with protected characteristics in the scope of this project / change / policy / procedure / practice / activity. Mitigation, where appropriate has been identified and dealt with accordingly.*

| *Equality Assessor:* | *Stuart Francis* | *Date:* | *28/01/2021* |
|---|---|---|---|

**Additional guidance**

| Protected characteristic | | Who to Consider | Example issues to consider | Further guidance |
|---|---|---|---|---|
| 1. | Disability | A person has a disability if they have a physical or mental impairment which has a substantial and long term effect on that person's ability to carry out normal day today activities. Includes mobility, sight, speech and language, mental health, HIV, multiple sclerosis, cancer | Accessibility<br>Communication formats (visual & auditory)<br>Reasonable adjustments.<br>Vulnerable to harassment and hate crime. | Further guidance can be sought from:<br>Solent Disability Resource Group |
| *2.* | Sex | A man or woman | Caring responsibilities<br>Domestic Violence<br>Equal pay<br>Under (over) representation | Further guidance can be sought from:<br>Solent HR Team |
| *3* | Race | Refers to an individual or group of people defined by their race, colour, and nationality (including citizenship) ethnic or national origins. | Communication<br>Language<br>Cultural traditions<br>Customs<br>Harassment and hate crime<br>"Romany Gypsies and Irish Travellers", are protected from discrimination under the 'Race' protected characteristic | Further guidance can be sought from:<br>BAME Resource Group |
| *4* | Age | Refers to a person belonging to a particular age range of ages (eg, 18-30 year olds) Equality Act legislation defines age as 18 years and above | Assumptions based on the age range<br>Capabilities & experience<br>Access to services technology skills/knowledge | Further guidance can be sought from:<br>Solent HR Team |
| *5* | Gender Reassignment | " The expression of gender characteristics that are not stereotypically associated with ones sex at birth" World Professional Association Transgender Health 2011 | Tran's people should be accommodated according to their presentation, the way they dress, the name or pronouns that they currently use. | Further guidance can be sought from:<br>Solent LGBT+ Resource Group |
| *6* | Sexual Orientation | Whether a person's attraction is towards their own sex, the opposite sex or both sexes. | Lifestyle<br>Family<br>Partners<br>Vulnerable to harassment and hate crime | Further guidance can be sought from:<br>Solent LGBT+ Resource Group |
| *7* | Religion and/or belief | Religion has the meaning usually given to it but belief includes religious and philosophical beliefs, including lack of belief (e.g Atheism). Generally, a belief should affect your life choices or the way you live for it to be included in the definition. (Excludes political beliefs) | Disrespect and lack of awareness<br>Religious significance dates/events<br>Space for worship or reflection | Further guidance can be sought from:<br>Solent Multi-Faith Resource Group<br>Solent Chaplain |
| *8* | Marriage | Marriage has the same effect in relation to same sex couples as it has in relation to opposite sex couples under English law. | Pensions<br>Childcare<br>Flexible working<br>Adoption leave | Further guidance can be sought from:<br>Solent HR Team |
| *9* | Pregnancy and Maternity | Pregnancy is the condition of being pregnant or expecting a baby. Maternity refers to the period after the birth and is linked to maternity leave in the employment context. In non-work context, protection against maternity discrimination is for 26 weeks after giving birth. | Employment rights during pregnancy and post pregnancy<br>Treating a woman unfavourably because she is breastfeeding<br>Childcare responsibilities<br>Flexibility | Further guidance can be sought from:<br>Solent HR team |