

## Crime Prevention Policy

Issue Date	Review Date	Version
February 2021	February 2026	3

### Purpose

The purpose of this policy is to:

- Ensure the best protection at all times for staff, patients, and visitors.
- Ensure the protection of Trust premises from malicious acts of damage or trespass.
- Ensure the protection of Trust assets from fraud, theft, or damage.
- Provide suitable advice with regard to the protection of personal property of staff, patients and visitors whilst on Trust premises.
- Ensure that effective and realistic improvements are made to security service provision.

### Who should read this document?

All staff with responsibility for the delivery security standards. Key roles:

- Chief Executive
- Director of Planning and Site Services (Director of Security)
- Matrons and Heads of Department

It will be the responsibility of these staff, to ensure that the contents of this policy are brought to the attention of all Trust staff and the staff of all organisations contracted to or volunteering to deliver services across the Trust.

### Key Messages

The security of the hospital site and the safety of those who use it is the responsibility of all of us.

ID badges need to be worn at all times and access authorisation properly controlled.

If you have concerns about a person or situation, please contact Saba Security via Helpdesk on 32000.

If an emergency response is required, call 3333.

Keys need to be controlled and checked daily to ensure they are returned.

Core accountabilities	
Owner	Local Security Management Specialist
Review	Health and Safety Committee
Ratification	Director of Planning and Site Services (Director of Security)
Dissemination (Raising Awareness)	Local Security Management Specialist
Compliance	Health and Safety Committee

### Links to other policies and procedures

--	--

### Version History

1	August 2012	New document created
2	October 2015	Updated and Reviewed
3	February 2021	Updated with name changes

*The Trust is committed to creating a fully inclusive and accessible service. Making equality and diversity an integral part of the business will enable us to enhance the services we deliver and better meet the needs of patients and staff. We will treat people with dignity and respect, promote equality and diversity and eliminate all forms of discrimination, regardless of (but not limited to) age, disability, gender reassignment, race, religion or belief, sex, sexual orientation, marriage/civil partnership and pregnancy/maternity.*

**An electronic version of this document is available on Trust Documents.  
Larger text, Braille and Audio versions can be made available upon  
request.**

## Contents

<b>Section</b>	<b>Description</b>	<b>Page</b>
1	Introduction	
2	Purpose, including legal or regulatory background	
3	Definitions	
4	Duties	
5	Key Elements	
6	Overall Responsibility for the Document	
7	Consultation and Ratification	
8	Dissemination and Implementation	
9	Monitoring Compliance and Effectiveness	
10	References and Associated Documentation	
Appendix 1	Dissemination Plan and Review Checklist	
Appendix 2	Equality Impact Assessment	

## 1 Introduction

University Hospitals Plymouth NHS Trust aims to provide a safe and secure environment for patients, visitors and staff providing and accessing the services delivered from Derriford Hospital and associated sites.

The policy sets out clear guidelines for Trust staff in order that they can anticipate, recognise, and appraise a crime risk, and then initiate an action to remove or reduce it.

The Trust manages major risks through a risk register held on the Trusts Risk management and reporting system (DATIX). This policy document identifies key responsibilities for ensuring that these risks are identified, monitored and controlled, and that the policy is implemented.

## 2 Purpose

### Purpose

The purpose of this policy is to:

- Ensure the best protection at all times for staff, patients, and visitors.
- Ensure the protection of Trust premises from malicious acts of damage or trespass.
- Ensure the protection of Trust assets from fraud, theft, or damage.
- Provide suitable advice with regard to the protection of personal property of staff, patients and visitors whilst on Trust premises.
- Ensure that effective and realistic improvements are made to security service provision.

### Scope

This policy applies to all Staff employed at University Hospitals Plymouth NHS Trust.

The policy also applies to all Staff not employed by the Trust, but who work on the University Hospitals Plymouth NHS Trust sites. This includes MOD, Hotel Services, Saba, as well as any Contractors who are engaged by the Trust.

This policy is applicable to all buildings and grounds of all University Hospitals Plymouth NHS Trust operated buildings and sites.

The Policy also applies to any location which houses Trust owned equipment of assets.

### Regulatory Background

There is no specific legislation that relates to this Policy.

Secretary of State for Health's Directions to NHS Bodies on Security Management Measures 2004.

## 3 Definitions

Crime Prevention is the anticipation, recognition and appraisal of a crime risk and the initiation of action to remove or reduce it.

**Chief Executive**

The Trust Board has overall responsibility for ensuring that the Trust meets its statutory obligations and that effective security arrangements are in place and periodically reviewed.

The Trust Board have responsibility for approving the Annual Security Review and for ensuring that any changes to the Security Management Director are notified to the NHS SMS within 7 days of the change.

**Director of Planning and Site Services (Director of Security)**

The role of the Director of Security is a statutory requirement for all Trust's as defined in the Secretary of State for Health's Directions to NHS Bodies on Security Management Measures 2004. The role is undertaken by a suitable Trust Executive Director who has responsibility for operational and/or strategic security matters. In this Trust the Director of Planning and Site Services is the nominated Director of Security.

The Director of Security is responsible for ensuring that there is a comprehensive assessment of the Risk associated with the physical premises and assets held in DATIX, and that these Risks are subject of a quarterly review and have appropriate mitigations and action plans in place.

The Director of Security is responsible for appointing the Local Security Management Specialist and ensuring that the LSMS remains appropriately qualified.

The Director of Security has final responsibility for ensuring that Security Risks associated with the physical security of the premises and assets are appropriately documented and managed, and that action plans are delivered to mitigate these risks.

**Local Security Management Specialist**

The Local Security Management Specialist has specific responsibility for Security matters within the Trust and to ensure that a consistent approach is adopted towards the provision of Security advice and monitoring. The LSMS discharges the role as defined in the Secretary of State for Health's Directions to NHS Bodies on Security Management Measures 2004.

The LSMS is responsible for the day to day management of the Risk Register (held in DATIX) that is associated with the physical security of the premises and assets, and that appropriate Risk Assessments are carried out.

The LSMS is responsible for ensuring that processes are in place to develop, deliver and monitor action plans associated with the physical security of premises and assets.

The LSMS is responsible for the production of the Annual Security Report for the Trust, and for ensuring that all statutory responses associated with security are made in a timely and accurate fashion.

The LSMS is responsible for liaising with other local organisations on security matters, and will use this liaison to inform the Trusts management of building and premise risk.

## **Security Manager (Saba)**

Saba are contracted by the Trust to provide manned and electronic security services across the Trust Estate, In this capacity, Saba are responsible for the day-to-day management of frontline risks associated with the security of the premises and assets.

The Security Manager (Saba) leads the Security Team and has responsibility for delivering the Security related components of the Integrated Car Parking & Security Management Services Contract.

The Security Manager (Saba) will promote a proactive response to the security of the premises and assets, ensuring that the security team:

- Leaving notes of personal items which have not been secured, reminding the owner that they could easily have been stolen.
- Report to the Trust LSMS doors which have been left wedged open, compromising security
- Undertaking poster and internal communication campaigns to raise awareness and promote improvements to security.

## **Matrons and Heads of Department**

Matrons and Heads of Department are responsible for:

- The development and adaptation of Trust Security procedures to ensure that they are relevant to specific Directorate / Departmental needs.
- Overall supervision of the day to day security measures within their Directorate or Department.
- Ensuring that any incident of crime or suspected crime is brought to the attention of the Saba Security Team.
- Ensuring that appropriate education and training is provided for all staff.

## **All Staff**

All members of staff have a responsibility to ensure that they comply with relevant Security policies and procedures. It is also essential that all Security incidents involving or observed by staff are reported in accordance with the Trust's incident reporting procedure. (DATIX)

## **5 Key Elements**

### **Policy Statement**

The Trust will support the delivery of high quality clinical services, through the provision of a secure environment and by protecting people and property from violence, damage, and theft.

There are three levels to the management of risk associated with premises and property:

- Risk Assessments associated with each of the premises that the Trust operates from, which covers security risks associated with the building.
- Risk Assessments associated with organisation wide risks which respond to cross cutting activities (such as Cash Collection) or emerging trends.
- Local Risk Assessments which cover the special security requirements associated with an area or activity.

The Trust will tackle Crime Prevention through a range of initiatives and approaches which are outlined below.

### **Building Related Risk Assessments: Reducing the Opportunity for Crime**

In order to reduce the Opportunity for Crime, the Trust develops and manages a suite of Risk Assessments associated with each building from which it operates. These Risk Assessments evaluate the physical environment and cover risks associated with:

- The location;
- The building fabric and layout;
- The activity carried out within the building;
- The security of assets

These Risk Assessments are reviewed annually by the LSMS, or when a significant change is made to a building. The resulting action plans from these Risk Assessments is used to shape the priorities for the Estates Strategy (long term) and Planned Maintenance Programme (medium term). Short term, high impact risks are incorporated into the Security Risk Register and the action plans agreed and monitored by the Health and Safety Committee.

### **Organisation & Responsive Risk Management**

Risk Assessments are also developed for organisation wide and emerging risks, such as those arising from:

- Organisation wide activities
- Communication cascade from the NHS SMS
- Local liaison activities of the Director of Security and the LSMS.
- Local police alerts
- Alerts from other NHS sites
- Saba intelligence from other sites where they deliver security services
- Concerns from staff raised through internal communication channels and flagged to the LSMS
- Crime pattern analysis carried out by Saba and the LSMS

When a new risk is identified, it will be discussed at the monthly Contract Review Group meeting in order to understand the risk, develop the risk assessment, and the associated risk mitigation action plan. The LSMS is responsible for ensuring that the risk is entered onto DATIX and that the action plan is logged so that progress can be tracked. Progress in delivering the action plan will be reported to and monitored by the Health and Safety Committee.

Local Risk Assessments: Department Managers are accountable for the assessing the risks within their areas. This includes carrying out risk assessments on the physical security of their areas and assets.

The LSMS is available to support the production of these local Security Risk Assessments. Where actions which require security improvements are identified as a result of these Risk Assessments, the LSMS should be notified. The LSMS will work with Departmental Managers to ensure that these actions are complete, and if necessary, capture the risks and actions on the organisational Security Risk Register.

To support the mitigation of Trust premises and asset security, all staff are asked to be vigilant:

- If any member of staff observes anyone acting suspiciously they should contact the Security Team (Saba) on Extension 39020 (or via the Saba Helpdesk on 32000)
- Staff should not challenge or place themselves at risk unless there is a clear threat of injury to colleagues, patients or visitors.
- Contractors and Suppliers will be informed of the Trust's Security Policies and Procedures, and must comply.

The following sections describe some of the control measures that staff should be aware of in relation to the most common sources of premises and asset related security risks.

### **Crime Pattern Analysis**

The Security Manager (Saba) will analyse the information and will report this analysis to the Integrated Car Parking & Security Contract Review Meeting. This Group will use this analysis to identify improvements to the security measures. In addition this data will be included will be used to update the Risk Register for Security held on DATIX.

Internal Communications routes will be used to promote Crime Reduction initiatives based on these analyses.

To support this, all staff should ensure that near misses and security breaches are reported to the Saba Security Team and entered in DATIX. This will allow the Trust to understand not only the patterns of crime, but also be able to target the most common security lapses that lead to criminal activity.

### **Cash Security**

The presence of cash anywhere on site represents a security risk. The sections below describe the approaches that should be used to minimise these risks in different situations.

#### **Non-patients**

All cash should be held in a safe or in a lockable cash box which would normally be deposited in a safe for storage.

Only one key to the safe should be retained in the department. If a duplicate key is required this should be held in a manner approved by the Director of Finance. Keys to safes should be securely held and issued only to those staff requiring access.

If a key to a safe is lost, the loss should be reported to the Director of Finance. Duplicate keys can only be obtained with the permission of the Director of Finance.

Staff responsible for the receipt and banking of cash should be familiar with and adhere to the University Hospitals Plymouth NHS Trust's Standing Financial Instructions.

Any movement of cash between departments in amounts greater than £50 should be done so only with security personnel present. To obtain an escort, telephone The Saba Helpdesk on Extension 32000 and inform time/date/place of escort.

Staff should be discouraged from bringing large amounts of personal cash to work. The Trust accepts no responsibility for any personal cash lost or stolen whilst on Trust premises.

### **Patients**

Patients should be advised not to bring valuables into the hospital, and anything of significant value should be removed by the patient's relative or guardian. Where this is not possible, a record of the patient's property must be completed by a member of hospital staff in the presence of a second member of staff and of the patient or his/her personal representative where practicable.

It is not recommended for patients to hold more than £10 on the Ward.

A full description of the processes for handling and securing patient's property are given in TRW.PAS.POL.465.1: Management of Patients' Property.

### **Contractors**

Both Saba (Car Parking, Security & Grounds Services) and Hotel Services operate services which involve the collection of cash.

### **Theft of Trust Assets**

It is a criminal offence to remove any property belonging to the Trust without permission from the appropriate Ward/Department. If you are aware of an incident of this type:

- Contact the Security Department immediately through the Saba Helpdesk on 32000.
- Complete a Trust Risk Management Incident Form (DATIX)
- In addition the Departmental Manager/Ward Sister must comply with the procedure for reporting losses as detailed in University Hospitals Plymouth NHS Trust Standing Financial Instructions.

The Saba Security Team will carry out regular campaigns as part of their internal patrols and night time lockdown, to identify Trust assets which could have been stolen. The Saba team will keep records of where they have identified such security risks, and will inform the LSMS of patterns of repeat incidents.

Such repeat incidents will be entered in DATIX and assigned to the Directorate Manager. This will ensure that a local action plan is developed. The Trust's Directorate Management Dashboards will be used to monitor progress against open actions.

### **Building Security**

Managers are responsible for ensuring that there are suitable arrangements for securing premises. The following safety checks must be carried out:

- Check that all areas are vacated (incl. toilets/rest rooms).
- Ensure that all lights and electrical appliance are switched off.
- Check that all doors and windows are locked – even if leaving for a short time.
- Secure key-operated window. (Burglars don't like breaking glass because of the noise and the risk of leaving forensic evidence.)
- Switch the burglar alarm on! (if appropriate)

- Ensure that Computers and other valuables cannot be seen from the window and are not at arm's reach.
- Ensure that Staff never leave the building/office via the fire exit

Saba Services are responsible for the lockdown of the hospital at night, and checking the security of all areas (as described in their Method Statement).

### **Portable Equipment Security**

Managers are responsible for ensuring that there are suitable arrangements for securing equipment. The following checks must be carried out:

- All equipment when not in use should be stored in a secure area.
- Make/Serial number and Model number for all equipment should be recorded on an Inventory when purchased Equipment managed by MEMS and all corporate IT equipment will form part of a centrally held inventory. All other equipment should form part of a local inventory.
- Inventories and records should be checked by a senior member of staff on an annual basis. Inventory records should be kept up to date and reviewed by the Departmental Manager on a regular basis.
- Do not store equipment in highly visible areas i.e. in front of windows, behind counters etc.
- Equipment, where appropriate, should be security marked. Request for security marking should be made to the Security Control on Extension 32000.
- Use security brackets whenever possible. For further advice, please contact the Security Manager on Extension 32000.
- All computer equipment should be secured by a suitable physical security device. All IT equipment and consumables should comply with the Trust's IT Security policies. Further information is available from the IT Service desk.
- Staff should be discouraged from bringing personal equipment onto Trust premises. University Hospitals Plymouth NHS Trust does not accept responsibility for losses or damage of personal equipment belonging to staff.
- Loans of equipment to other Trust Staff/Departments should be properly documented and monitored.
- Staff should be aware of and adhere to University Hospitals Plymouth NHS Trust's Financial Instructions concerning the Security of Assets.

### **Tampering with equipment**

All equipment is at risk of being tampered with. This can pose a significant risk to those who use such equipment, and also those who the equipment is used on.

Portable equipment should be stored securely whilst not in use. Very sensitive equipment which cannot be moved should have security locks fitted to control where possible.

In any event, staff should check equipment thoroughly before use for signs of tampering. All equipment settings should be checked, and it should not be assumed that uncommonly used controls are correctly set.

Staff should report any incidents of equipment tampering through DATIX, so that the appropriate investigation can be carried out, and that trends are captured and monitored.

## **Key Security**

### External Doors

- All keys to external doors will be held centrally in the Saba Security Control Room and are accessible 24 hours a day. Keys will only be issued on production of a valid University Hospitals Plymouth NHS Trust Photo ID Badge. All keys will be signed in/out.
- Extra keys must not be cut without the authorisation of the Local Security Management Specialist. The unauthorised cutting or holding of keys will be regarded as a disciplinary offence.
- Key Access Control Lists for restricted buildings are to be updated by the Departments concerned on a regular basis and held within the Saba Security Control.

### Internal Doors

- All keys to internal doors should be clearly marked - tagged (by number rather than description).
- Internal records should be kept to identify each key and corresponding lock.
- All keys should be securely stored when not in use, and access limited.
- Staff must not take departmental keys off site outside normal working hours.
- The issue and receipt of keys must be controlled and a 'Daily Key Check' should be carried out to ensure that all keys are accounted for. This check should be carried out by all those holding Keys on behalf of the Trust
- Any lost keys should be reported, in the first instance, to the Saba Security Manager.
- The cutting of internal keys must be authorised by the Departmental Manager.

## **Access Controls**

For access systems to be effective, it is necessary to ensure that robust measures are in place. The most effective method of controlling access is to restrict the number of Authorisers. Ideally there will be one Door Access Card Authoriser per speciality/department, with a named deputy to cover in case of absence.

- The Door Access Card Authorisers should be Management grade staff (Band 6 or above)
- The Door Access Card Authoriser will complete and sign an ID Badge Request Form providing the following information:
  - Name of person requiring access card (Full name no nicknames)
  - Job title/department of person requiring access card
  - Employer (i.e.: Trust, MOD, Hotel Services etc.)
  - Date of Birth of person requiring access card
  - Date of expiry (if appropriate)
  - Areas to which access is required (building/room etc.)
  - Name, job title and department of Authoriser
  - Signature of Authoriser

- Cards are issued by Saba, who are responsible for preparing the photographs and printing the cards. Cards will only be programmed for access as detailed on the ID Badge request.
- Cards belonging to those leaving the Trust will be automatically cancelled by Saba. However used badges must be returned (by the Line Manager) to the Saba Security Office for destruction. Saba will reconcile cards received with the leavers list, and alert the LSMS to discrepancies. The LSMS will approach the appropriate Directorate to ensure that leaver's cards are recovered.

### **Access Control – Key Pads**

Where key pads are used on external doors, the code should be advised to the Security Department.

Codes should only be divulged to staff 'who need to know' and staff must not disclose the codes to any other persons.

Under no circumstances must door codes be displayed.

Where appropriate, codes should be changed on a regular basis.

Before a key pad is purchased, advice should be sought from the Local Security Management Specialist.

Override keys should only be held by the Trusts LSMSs, Saba and the Estates team.

### **Other Keys**

Keys to padlocks, cupboards, filing cabinets etc. should also be controlled. It is recommended that:

- Keys are held centrally in a lockable key cupboard and issued only to personnel requiring access.
- Keys should be clearly tagged and labelled.
- At the end of each working day all keys must be accounted for.
- Staff should be discouraged from taking keys home or carrying them during the day.
- The number of duplicate keys should be kept to a minimum and controlled.

### **Identification Badges (ID)**

All staff must wear an official Trust Photo-ID Badge in a prominent position whilst on duty in line with the Trust ID Policy.

New starters must produce an ID Badge Request Form completed by their Line Manager/Human Resources before an ID badge can be issued.

Existing staff already in possession of a Trust ID Badge and requiring a replacement must email the staff ID mailbox requesting a new badge and providing details of why this is required. Requests for change of name or job title must come from the member of staff's line manager.

Staff must collect their ID badge from the Security Control in person. ID badges will not be given to third parties under any circumstances.

All staff, on commencement of their employment, should request a temporary ID Pass from the Security Office until an official ID Badge has been produced.

Short-term, temporary staff should request a temporary ID Badge from the Security Office. This will apply to the following categories: Locum, Agency and short-term temporary staff attending on an infrequent basis.

Where applicable, an expiry date/contract end date should be detailed on the ID Badge Request Form, for inclusion on the ID Badge.

ID Badge Request Forms are available to Line Managers only, and must be completed in full and signed by the Line Manager prior to issuing.

Leavers must return their ID Badges to their Line Manager on their last working day. It is the responsibility of the Line Manager to ensure that the ID Badge is recovered, and returned to the Security Department for logging and destruction.

ID Badges with door access will be monitored on a regular basis (bimonthly) and lists of cardholders sent to Departmental/Ward Managers for confirmation.

Cards are issued by Saba, who are responsible for preparing the photographs and printing the cards.

### **Contractors on Site**

If Contractors are to commence work on Trust premises, the relevant Departmental Manager must inform the ID team via the Contractor Mailbox, and the contractor must attend the ID session, when the ID badge will be produced for the contract period.

Short term contractors must obtain temporary passes from the Security Control

## **6 Overall Responsibility for the Document**

Local Security Management Specialist

## **7 Consultation and Ratification**

The design and process of review and revision of this policy will comply with The Development and Management of Formal Documents.

The review period for this document is set as default of five years from the date it was last ratified, or earlier if developments within or external to the Trust indicate the need for a significant revision to the procedures described.

This document will be reviewed by the Health and Safety Committee and ratified by the Director of Planning and Site Services.

Non-significant amendments to this document may be made, under delegated authority from the Director of Planning and Site Services, by the nominated owner. These must be ratified by the Director.

Significant reviews and revisions to this document will include a consultation with named groups, or grades across the Trust. For non-significant amendments, informal consultation will be restricted to named groups, or grades that are directly affected by the proposed changes.

## 8 Dissemination and Implementation

Following approval and ratification, this policy will be published in the Trust's formal documents library and all staff will be notified through the Trust's normal notification process.

Document control arrangements will be in accordance with The Development and Management of Formal Documents.

The document owner will be responsible for agreeing the training requirements associated with the newly ratified document with the named Director of Planning and Site Services and for working with the Trust's training function, if required, to arrange for the required training to be delivered.

## 9 Monitoring Compliance and Effectiveness

The Health and Safety Committee is the designated Trust Committee which provides oversight and governance of Security matters. The Health and Safety Committee is Chaired by the Director of Governance. The Table below described the approaches used for the monitoring of compliance and effectiveness. Outcomes from this monitoring are reviewed, considered and approved by the Health and Safety Committee.

What	Who	When	How
Ensuring that the Trust has an appropriately reviewed Security Risk Register and action plans are in place and updated	Director of Security	Six Monthly	Review and approval of Risk Register by Health and Safety Committee. Action plans reviewed and updated by the LSMS.
Ensuring that the Trust has reviewed and actioned any security related incidents	LSMS	Six Monthly	Report on Security Incidents. Report on outstanding actions arising. Audit of a sample of Security Incidents to check for completeness.
Ensuring that all staff have received appropriate security Training	Director of HR&OD	Induction & Annual	To be covered within Annual Appraisals. Audit of training records.
Ensuring the Security Incidents are reported in DATIX correctly	LSMS	Annual	Audit of a sample of DATIX incidents. Survey of staff to ensure they understand how to report incidents correctly.

All staff are aware of the contents of this Policy	LSMS	Six Monthly	Survey of staff to ensure they understand the requirements of this Policy.
The issue of security passes are appropriately authorised	Saba/HR	Quarterly Annual	Audit against IPSMS (Saba) Contract KPIs Audit of Security Pass Database, comparing with HR data.
Passes are destroyed upon the staff member leaving the Trust	Saba	Quarterly	Reconciliation between leavers lists and passes returned for destruction.
Site is locked down appropriately in quiet hours	Saba	Monthly	Monitoring of Saba Contract KPIs
Equipment is checked for signs of tampering	LSMS	Six Monthly	Audit of incident reports. Observational audits in high risk areas
Site patrols are carried out to identify security risks	Saba	Daily	Monitoring of Saba Contract KPIs
Near miss reporting of security breaches is recorded in DATIX	LSMS	Annually	Review of Near Miss coverage – to identify gaps.
All staff must wear ID badges and challenge those in staff areas who are not wearing one	LSMS	Six Monthly	Observational audit
Appointment letters advise patients to leave valuables at home	Patient Services	On-Going	Audit of sample of letters
Staff adhere to TRW.PAS.POL.465.1 (Improving the Patient Experience – 3. The Handling of Patients' Property)	LSMS	On-Going	Observational audit.
Staff involved in cash handling adhere to local cash handling policies and the Trust	Finance / Matrons	On-Going	Review of partner organisations Cash Handling Policies

Standing Financial Instructions			Audit of compliance with policies,
---------------------------------	--	--	------------------------------------

In addition, the LSMS will produce an Annual Security Report which will be approved by the Health and Safety Committee, before being ratified by the Trust Board and submitted to NHS Protect for External Validation.

Any changes to key Security Staff (Security Executive Director, Non-Executive Director with responsibility for Security and LSMS) will be approved by the Trust Board, and to the NHS SMS as appropriate.

**10 | References and Associated Documentation**

**Further Advice**

Further Advice is available from the Local Security Management Specialist

**Useful Telephone Numbers:**

- 3333                      Switchboard (Emergency)
- 39738 or 37004        Local Security Management Specialist (LSMS)
- 32000                    Saba Helpdesk
- 0240                      Security Fast Bleep

Dissemination Plan			
<b>Document Title</b>	Crime Prevention Policy		
<b>Date Finalised</b>	February 2021		
Previous Documents			
<b>Action to retrieve old copies</b>	Remove from Staffnet		
Dissemination Plan			
Recipient(s)	When	How	Responsibility
All Trust staff		Information Governance StaffNet Page	Information Governance Team

Review Checklist		
<b>Title</b>	Is the title clear and unambiguous?	Yes
	Is it clear whether the document is a policy, procedure, protocol, framework, APN or SOP?	Yes
	Does the style & format comply?	Yes
<b>Rationale</b>	Are reasons for development of the document stated?	Yes
<b>Development Process</b>	Is the method described in brief?	Yes
	Are people involved in the development identified?	Yes
	Has a reasonable attempt has been made to ensure relevant expertise has been used?	Yes
	Is there evidence of consultation with stakeholders and users?	Yes
<b>Content</b>	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
<b>Evidence Base</b>	Is the type of evidence to support the document identified explicitly?	Yes
	Are key references cited and in full?	Yes
	Are supporting documents referenced?	Yes

<b>Approval</b>	Does the document identify which committee/group will review it?	Yes
	If appropriate have the joint Human Resources/staff side committee (or equivalent) approved the document?	n/a
	Does the document identify which Executive Director will ratify it?	Yes
<b>Dissemination &amp; Implementation</b>	Is there an outline/plan to identify how this will be done?	Yes
	Does the plan include the necessary training/support to ensure compliance?	Yes
<b>Document Control</b>	Does the document identify where it will be held?	Yes
	Have archiving arrangements for superseded documents been addressed?	Yes
<b>Monitoring Compliance &amp; Effectiveness</b>	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
<b>Review Date</b>	Is the review date identified?	Yes
	Is the frequency of review identified? If so is it acceptable?	Yes
<b>Overall Responsibility</b>	Is it clear who will be responsible for co-ordinating the dissemination, implementation and review of the document?	Yes

<b>Core Information</b>	
<b>Date</b>	February 2021
<b>Title</b>	Crime Prevention Policy
<b>What are the aims, objectives &amp; projected outcomes?</b>	To ensure a secure environment for staff, patients and visitors and comply with legislation, guidance, best practice and Trust policies.
<b>Scope of the assessment</b>	
<b>Collecting data</b>	
<b>Race</b>	No
<b>Religion</b>	No
<b>Disability</b>	No
<b>Sex</b>	No
<b>Gender Identity</b>	No
<b>Sexual Orientation</b>	No
<b>Age</b>	No
<b>Socio-Economic</b>	No
<b>Human Rights</b>	No
<b>What are the overall trends/patterns in the above data?</b>	No data has been collected during this review.
<b>Specific issues and data gaps that may need to be addressed through consultation or further research</b>	None

<b>Involving and consulting stakeholders</b>				
<b>Internal involvement and consultation</b>	Members of the Trust's Health and Safety Committee including JSNC representatives and Trust's Security Management Specialist and Director of Security.			
<b>External involvement and consultation</b>				
<b>Impact Assessment</b>				
<b>Overall assessment and analysis of the evidence</b>				
<b>Action Plan</b>				
<b>Action</b>	<b>Owner</b>	<b>Risks</b>	<b>Completion Date</b>	<b>Progress update</b>