NHS Lothian

Title: **NHS Lothian Physical Security Policy**	
Date effective from: September 2023	**Review date:** September 2026
Approved by:	Policy Approval Group
Approval Date:	5 September 2023
Author/s:	Head of Risk, Quality & Assurance (Estates & Facilities) Lead for Security and Car Parking (Estates & Facilities) Site Services Manager (Estates & Facilities) Head of Soft FM (Estates & Facilities) Key Contributors: NHS Lothian Security Committee
Policy Owner:	Director of Operations (Estates & Facilities)
Executive Lead:	Deputy Chief Executive
Target Audience:	All NHS Lothian staff
Supersedes:	New policy
Keywords (min. 5):	Security, CCTV, Safety, Crime Prevention, Theft, Vandalism, Counter Terrorism, Access control

NHS Lothian Physical Security Policy

Version Control

Date	Author	Version/Page	Reason for change
July 2021	Head of Soft FM (Estates & Facilities)	v0.1-2	New policy under development
June 2023	Head of Risk, Quality & Assurance Lead for Security and Car Parking Site Service Manager Soft FM Head of Soft FM	v0.3-4	Update to include recommendations from the Security Review leading to submission into the governance process.
Sept 2023	Head of Risk, Quality & Assurance Lead for Security and Car Parking Site Service Manager Soft FM Head of Soft FM	v1.0	Approved by the Policy Approval Group

Executive Summary

This policy aims:

- To ensure that we can provide a secure and safe environment within which our staff can provide all the services necessary for the delivery of healthcare.

- To establish the procedures which we will use as far as possible to safeguard our staff, patients and the public and our assets against any threat, loss, theft, damage or disruption.

- The prevention of crime to persons and property including activities which could cause a physical risk to staff, service user, property or our reputation.

- To ensure compliance with the required Security Services Standards.

- To implement the recommendations from the 2022 NHS Lothian Security Review

NHS Lothian will adopt a proactive approach in providing the level of protection necessary to achieve the above aims, adopting an approach that includes; ensuring a security culture and a suitable level of security awareness among all levels of staff through progression of the recommendations from the Security Review; the provision and maintenance of security systems deemed necessary, following the appropriate risk assessment process; and ensuring a high level of competency of all staff directly engaged in the provision of security services.

NHS Lothian Physical Security Policy

Contents

1.0   Purpose

The main aims of this policy are:

- To ensure that we can provide a secure and safe environment within which our staff can provide all the services necessary for the delivery of healthcare.

- To establish the procedures which we will use as far as possible to safeguard our staff, patients and the public and our assets against any threat, loss, theft, damage or disruption.

- The prevention of crime to persons and property including activities which could cause a physical risk to staff, service user, property or our reputation.

- To ensure compliance with the NHS Assure Security Services Standards.

2.0   Policy statement

NHS Lothian will adopt a proactive approach in providing the level of protection necessary to achieve the above aims. This approach will take the form of *Deter, Deny, Detect and Respond* including:

- The appointment of an Executive Lead for Security;

- The appointment of a Lead Security Adviser with an appropriate level of experience/competence which will be maintained;

- Ensuring a security culture and a suitable level of security awareness among all levels of staff through progression of the recommendations from the Security Review;

- The provision and maintenance of security systems deemed necessary, following the appropriate risk assessment process;

- Ensuring a high level of competency of all staff directly engaged in the provision of security services;

- Ensuring legislative compliance in relation to duties and responsibilities;

- Ensure that this policy and the processes which are put in place from it are effectively communicated, and are reviewed for effectiveness.

We will cooperate with Police Scotland including for the prompt and accurate reporting of incidents, consultation on all aspects of security provision ensuring we adopt best practice and making best use of any security review/audit services they or other associated bodies provide.

3.0   Scope

All NHS Staff and covering all sites

This policy does not cover:

- Fire (see NHS Lothian Fire Safety Policy)

- Controlled stationery (other than in relation to the area within which such documents are stored)

- Information or data security (see NHS Lothian Records Management Policy, available on the NHS Lothian intranet)

- Fraud (see NHS Scotland Workforce Conduct Policy and NHS Lothian Standing Financial Instructions).

- **Note**: there are other policies linked with this policy as defined in section 6 and referenced throughout the policy. It is recommended they are read in conjunction with this policy.

4.0   Definitions

For the purposes of this policy the term "security" will be defined as the risk of disruption to service to NHS Lothian arising out of:

- Injury to persons ref Adverse Event Management Procedure,

- Missing persons; as per local site procedures

    - RIE Missing Patient Procedure, Engie, February 2020

    - Patients who absent themselves from Adult Inpatient Services, Royal Edinburgh Hospital (Joint Protocol), NHS Lothian (REH)/Police Scotland, November 2017

    - Standard Operating Procedures for Reporting Missing Persons from Adult & Older People's Mental Health In-patient Services Royal Edinburgh Hospital, approved by Adult And Older People's Mental Health Executives, January 2020

    - Acute Partnership Agreement, NHS Lothian/Police Scotland, June 2021

    - Protocol for Missing Persons In Patient Services, St John's Hospital

- Access to areas where a person could become confused, lost, isolated, trapped or find themselves in a potentially dangerous situation;

- Damage to property including buildings and external areas;

- Inappropriate access to specific service areas e.g. Pharmacy, Children's Units, or Cashiers offices etc;

- Theft of or damage to our equipment or infrastructure;

- Removal of safety or directional signage

- Theft of personal property;

- Loss of keys or access cards

5.0   Implementation roles and responsibilities

5.1   Staff responsibilities

5.1.1 Director of Operations (Estates & Facilities)

Management of Security is delegated to the Director of Operations (Estates & Facilities) by the Executive Lead for Security (Depute Chief Executive) who is tasked with ensuring that necessary arrangements are in place in all areas. This includes carrying out security risk assessments and taking forward the outcomes from these to ensure that all risks in relation to security are adequately controlled.

A nominated competent person (Lead for Security & Car Parking Estates and Facilities) is available for the provision of advice on security related matters.

5.1.2 Estates & Facilities Managers with a security service responsibility

Estates & Facilities Managers with a security service responsibility will:

- Have identified the staff to whom this policy applies

- Have identified and assessed the risks in this regard

- Have established suitable procedures to address the key risks

- Ensure suitable and specific training programmes are available to inform and support staff.

5.1.3 Estates & Facilities staff with a security service role

Estates & Facilities staff with a security service role will:

- Ensure that they have read the policy and any associated procedures and comply with the provisions within these

- Engage with any training that is provided

- Report all security incidents and maintain and protect accurate records relating to security incidents

- Co-operate with reasonable requests from recognised agencies e.g. Police

- Operate CCTV systems in accordance with established Information Governance principles and Information Commissioner's Office (ICO) guidance.

- Assist staff in locating missing patients

- Assist custodial staff or Police Scotland with searches where appropriate

5.1.4 Managers and staff from all other departments

- Will ensure that they have read the policy and any applicable procedures and comply with these

- Will have locally assessed any security related risks taking guidance where needed

- Comply with any reasonable requests relating to security procedures, investigations and improvements.

5.1.5 All staff

Have a responsibility for ensuring general compliance with the terms of this policy. This includes maintaining security awareness and assessing security risks impacting within their own service. All staff will ensure the maintenance of a secure environment for service delivery by their awareness of security risks and procedures.

5.1.6 Shared accommodation with partner organisations

Where we share accommodation with partner organisations including PFI/PPP sites, the senior NHS manager for the area will share the contents of this document to ensure that potential gaps and overlaps between our provisions and those of our partners are understood and managed appropriately.

5.2 Reporting and Monitoring Arrangements

Security incidents will be recorded on the DATIX system and a regular review of these will be undertaken locally in specific departments and as part of the work of the Security Committee. The findings will be included within the Local Health and Safety Committees, and the Health and Safety Quarterly Reports to the NHS Lothian Health and Safety Committee.

Security incidents will be reported to the local Security Office or Site Facilities Manager via the most appropriate method (telephone, email, teams call) and followed up on Datix and local reporting logs.

Significant security incidents including threats or injury to persons, missing persons, significant malicious damage to property or equipment must be reported to the police, and/or senior management, and a DATIX report logged.

5.3 General Security Provisions

5.3.1 Keeping People Safe - Staff

1. NHS Lothian takes the threat of violent incidents against staff very seriously. As effective security relies heavily on a team approach, each individual member of staff is expected to be aware of and comply with this policy and to implement the procedures contained herein as appropriate. Staff are expected to wear ID badges at all times Identification/Security Pass Application Form and to close windows and lock doors where possible at the end of the working day.

2. Staff who are actively involved in the provision of physical security or where there is a threat of physical violence, will be appropriately trained prior to commencing work, this will include violence and aggression training and other site-specific duties relating to security. Security staff where available will attend any security incident which poses a risk to staff, patients or visitors and will operate under the guidance of clinical staff.

3. Breaches of security which are observed by staff during their work must be reported immediately following the local management procedures for the area. All incidents involving aggression and violence must be reported to the local manager. NHS Lothian has a zero-tolerance attitude to such physical violence directed against its staff whether threatened or actual and will report any such incidents to the police and seek prosecution if appropriate.

4. Where used, agencies or contractors which supply us with staff or services will, where appropriate, have their employment processes verified for security. Suitable permits to work will be issued to contractor's staff when they are working in vulnerable or high-risk areas. Please see the NHS Lothian Control of Contractors Policy. Identification badges will always be worn and visible.

5.3.2 Keeping People Safe - Patients and Visitors

1. NHS Lothian will endeavour to provide safe and secure access for patients and visitors to the services it provides. Our staff will have the necessary knowledge to provide support to any visitor or patient who reports a security incident to them. In most circumstances this will involve directing/accompanying them to the local manager on duty who can complete the necessary reports.

2. Patients, their relatives and visitors will be informed of the local security arrangements by:

   – Department photograph boards

   – Verbal advice from staff

   – Effective wayfinding maps around our sites

3. We will always be willing to accept and respond to feedback to any visitor or patient concern on security matters

4. Where a patient/visitor area is considered to be vulnerable following risk assessment, such as those areas providing services to children, or pharmacy areas a high priority will be given to improving security in this area. These areas will be identified by local risk assessment by the Senior Department /Service Managers and reviewed regularly or after incident.

5. Missing Patients: The management of in and outpatients is the responsibility of the clinical department with control over the case. Where there is an incident of a patient missing from healthcare premises contact local site bleep holder and security office for local site procedures.

6. Where a patient absconds and in under custodial supervision please refer to: Security and Supervision of Prisoners Receiving Treatment in NHS Lothian Hospitals,

5.3.2.1 Property and Systems

5.3.2.2 Buildings

All buildings will be formally and informally risk assessed by all departmental managers on a regular basis in relation to security. This will include the factors below assessing the building from the point of view of:

- Services provided and ease of access to services including effective wayfinding

- Requirement for access, internal subdivisions and associated access control

- Points of access including emergency access/egress

- Times of access and lockdown procedures

- Security systems available/required e.g. CCTV and Security access systems

- Proximity to other areas

- Access to roof areas, high spaces, restricted access areas etc.

- Plant rooms

- Housekeeping to reduce the potential for unobserved suspect packages

- Hidden areas, appropriate lighting etc

- Management of mail rooms ensuring secure delivery of mail

5.3.2.3 Car parks and external areas

- Risk assessments will be conducted by Estates & Facilities site managers and reviewed annually or after an incident. In addition, consideration will be given to removing excess shrubbery from green areas and to improvement of lighting where they cause or contribute to security risks. Patrol of external areas will be provided where appropriate by staff using body cameras.

- Consideration will also be given to the security risks associated with traffic routes through our major sites. Traffic management procedures will be implemented where appropriate and vehicles which are obviously abandoned will be removed from our premises in conjunction with the police.

5.3.2.4 Personal property including valuables

- Wherever cash is being transported, the Board's Standing Financial Instructions will apply. These instructions are available from the Finance Department. All areas of NHS Lothian will ensure that effective procedures are in place for the recording, safe storage and staff movement of cash and valuables, including those held on behalf of patients, around and between sites where this is an issue.

- Patients and staff will be advised to leave valuables at home where possible and to avoid having large amounts of cash in their possession whilst on our premises.

- Staff must make use of whatever secure storage is available to them for their valuables, including lockers or lockable drawers Where lockers are not available staff must take responsibility for their own belongings.

- Information and guidance on patients' valuables and or funds can be found in the Patients Funds and Valuables Procedure (available on the NHS Lothian intranet).

5.3.2.5 NHS Lothian property and equipment

− Managers must ensure that all moveable equipment particularly portable and desirable items such as televisions, media players and IT equipment belonging to the organisation is security marked and securely stored when not in use. Consideration should be given to maintaining an asset register of all such equipment which should be regularly updated to include all purchases, moves and disposals.

− Losses of such equipment should be appropriately recorded as a security incident and reported to the Site Manager or manager with local security responsibility for the area. Investigation of all such losses should be carried out thoroughly by the local manager and consideration given to implementing operational changes to avoid the risk of repetition.

− Losses of Property/Equipment Statistics will be collated and the information which is generated will be used to improve our procedures and the security of the environment.

5.3.2.6 Vehicles

For further detail on this please refer to the [Driving at Work Policy](#)

− Staff are responsible for any vehicle while it is in their use. It is an important aspect of our insurance policy for business vehicles that these are kept secure when not in use. They must therefore never be left open when unattended and all vehicle keys must be maintained in a secure environment with an appropriate authorisation and control mechanism in place for vehicle use and return. Where possible NHS vehicles must be parked on Health Board premises when not in use.

− Staff must always consider their personal safety when driving on NHS business. Care must always be exercised when parking or returning to a vehicle and where possible a well-lit parking area should be chosen. When carrying equipment or other cargo within the community or on other NHS business, must ensure that this is kept out of view when the vehicle is parked for however short a period.

− Where a vehicle has been fitted with an alarm or immobiliser, these must be activated when the vehicle is unattended.

5.3.2.7 Security systems

− Security systems such as those listed in this section are provided to enhance the security of the environment, help reduce the fear of and potential for crime to occur and in the case of CCTV, to monitor vulnerable areas. Such systems do not negate the need for good housekeeping practices. All staff within their areas are required to ensure that access to our premises is controlled, by ensuring doors and windows are closed, and where appropriate, locked to prevent easy access.

− Staff must also make appropriate use of all security equipment provided for them including the setting and un-setting of local alarm systems. In such

cases training in the relevant system will be provided. Misuse of such equipment by staff may result in disciplinary action being taken. Defects in the correct operation of security related equipment must be reported to the local Head of Department and Estates Department as a matter of urgency logging the date and time of the report.

– If staff consider that additional security systems are necessary in a particular area then a request must be made to the local manager who will arrange for a risk assessment to be carried out jointly by the site services manager. Records of security incidents will be required to underpin such a request and it is therefore important that such records are maintained accurately.

5.3.2.8 CCTV recording systems

– All CCTV recording systems and the images recorded on them will be kept in a secure environment. Procedures will be implemented to control access to these images under the provisions of the Data Protection Act and the CCTV Guidance for Accessing Images. All requests to view images must be made in writing and approved by a nominated manager. See NHS Lothian CCTV Policy.

5.3.2.9 Identity badges

– All staff are required to wear identity badges at all times. Lost badges must be reported to the Head of Department and a request for replacement made to the local security office. Any lost badges which contain access controls must be rescinded. Badges are available to all new employees at induction, must not be shared or transferred and must be available for scrutiny at any time if a reasonable request is made. They must also be surrendered to the Head of Department on leaving the employ of the organisation. See Identification/Security Pass Application Form (available on the NHS Lothian intranet)

5.3.2.10   Controlled access systems

– Controlled door access systems are deployed in several key areas where an additional level of security is required. Access into such controlled areas is the responsibility of the local Head of Department. A database of authorised staff must be maintained and reviewed as necessary with access rights withdrawn promptly where it is no longer required. Where access is gained using an alpha-numerical code a local procedure must be in place to ensure that such codes are regularly changed, minimum frequency annually. This can be achieved by contacting the local Estates helpdesk.

– Traffic management systems including car park barriers contribute to the security of our sites where they are in place. Staff requiring parking access should follow the application procedure. Those drivers who need to gain entry to areas of our sites controlled by barriers (other than public car parks) and who do not have a permit will be asked to identify themselves and their requirement to our security staff prior to being given access.

5.3.2.11   Key security

- The issuing, recovery, recording and security of departmental keys is the responsibility of Departmental Managers. Premises and individual departments vacated for any length of time must be secured from any form of unauthorised entry.

- Duplicate keys are only available following completion and authorisation of the appropriate documentation and must be maintained in a designated secure place for use in the event of an emergency.

- Keys should not be able to be identified easily. For example, colour coding is a secure method of identification providing the explanatory chart is stored separately from the keys themselves. Managers should keep a list of keys issued to staff and should ensure that they are returned prior to staff leaving.

- Managers need to consider whether to replace locks if keys are lost or not returned. Contractors should only be given keys if the manager/estates department can guarantee adequate supervision and a record of their staff permitted to be on site. The list must be kept by the manager in case of subsequent security incidents.

- Local key cabinets/safes must be kept locked and under controlled supervision

5.3.2.12   Other Specific Security Risks and Procedures

Procedures for specific security risks are available on the intranet as highlighted in blue below; it is recommended that these policies and/or procedures are read in conjunction with this policy..

These include:

- Bomb threats

- Child abduction, child restriction orders

- Managing aggressive behaviour Keeping People Safe: Management of Violence and Aggression Policy

- Lone Working Lone Working Policy

- Community Working

- Out of Hours Arrangements

- Procedure for Accessing CCTV Images (CCTV Guidance for Accessing Images)

- Adverse Event Management Procedure Adverse Event Management Procedure

- Missing Persons

- Identity Badges

- Panic and other alarms

- Post Room Threats

- Access to roofs, high spaces or places of potential entrapment

5.3.2.13   Action in the event of incident/loss/damage

− Any report of an incident involving loss or damage which is received should be referred to the local manager for appropriate action. In the case of serious incidents, the on-call arrangements for NHS Lothian should be invoked - contact local site bleep holder for local site procedures.

5.3.2.14   Police liaison

− In cases of emergency or serious security incidents i.e. where there are life threatening circumstances and where people are in immediate danger the procedure is to immediately call 999.

− There are several local points of contact with the police where advice on security matters can be sought. This information is available from the local Facilities office or via Site Liaison Groups

6.0   Associated materials

Other local procedures and supporting policies incorporating general security advice for staff listed below.

NHS Lothian CCTV Policy, approved by Information Governance Sub Committee, April 2018

Identification/Security Pass Application Form (available on the NHS Lothian intranet)

Adverse Event Management Procedure, approved by the Policy Approval Group, July 2018 (under review)

Keeping People Safe: Management of Violence and Aggression Policy, approved by the Policy Approval Group, June 2023

The Purple Pack: NHS Lothian Risk Assessment and Risk Reduction System (Violence & Aggression and Lone Working), approved by the NHS Lothian Health & Safety Committee, November 2021

Lone Working Policy, approved by the Policy Approval Group,

Lone Working Procedure, approved by the NHS Lothian Health & Safety Committee, April 2021

Driving at Work Policy, approved by the Policy Approval Group, June 2022

Patient Engagement Policy, approved by the Policy Approval Group, July 2021

SOP Interventions in General Inpatient Settings, approved by NMAHP Senior Leadership Group, December 2021

Missing Persons - As per local site procedures

− RIE Missing Patient Procedure, Engie, February 2020

− Patients who absent themselves from Adult Inpatient Services, Royal Edinburgh Hospital (Joint Protocol), NHS Lothian (REH)/Police Scotland, November 2017

     − [Standard Operating Procedures for Reporting Missing Persons from Adult & Older People's Mental Health In-patient Services Royal Edinburgh Hospital](#), approved by Adult And Older People's Mental Health Executives, January 2020

     − [Acute Partnership Agreement](#), NHS Lothian/Police Scotland, June 2021

     − [Protocol for Missing Persons In Patient Services](#), St John's Hospital

Out of Hours arrangements (including on call) – as per local site procedures

[Patients Funds and Valuables Procedure](#), NHS Lothian Head of Financial Control, November 2019 (available on the NHS Lothian intranet)

[NHS Lothian Control of Contractors Policy](#), approved by the Policy Approval Group, December 2021

[NHS Lothian Fire Safety Policy](#), approved by the Policy Approval Group, April 2022

[NHS Lothian Records Management Policy](#), approved by the Information Governance Assurance Board, February 2018 (available on the NHS Lothian intranet)

[NHS Scotland Workforce Conduct Policy](#), June 2023

[Security and Supervision of Prisoners Receiving Treatment in NHS Lothian Hospitals](#), approved by the Clinical Policy Group, 2015

7.0   Evidence base

[SHFN 03-02](#) Security Services Standards for NHS Scotland Security Leads (v3.0 July 2021).

[Security Management Framework for NHS Boards in Scotland](#) (Dec 2008)

[Scottish National Security Management Framework (SHFN 03-01, 2008)](#)

[Health and Safety at Work etc. Act 1974](#)

8.0   Stakeholder consultation

This policy has been developed in consultation with stakeholders including the Estates & Facilities Soft FM Area Managers (responsible for Security Teams), NHS Lothian Security Committee, and the Estates & Facilities Policy Review Group.

A draft of this policy was placed on the NHS Lothian Consultation Zone to give NHS Lothian staff an opportunity to provide feedback.

9.0   Monitoring and review

This policy will be reviewed, as a minimum, every three years, but may be subject to earlier review in the event of changes in best practice, guidance or legislation, results from performance reviews and audits, or any other factors that may render the policy in need of review.

Good practice requires regular and frequent monitoring of compliance with this policy.

These will be monitored by the Lead for Security and Car Parking and the Security Committee

The effectiveness of this policy may also be monitored and evaluated using the outputs from:

- Annual risk assessment reviews and updates
- Monitoring of security logs
- SAE Reviews
- DATIX investigations
- Complaint investigations/improvement plans
- Health & Safety Quarterly Reports (compliance with relevant policies/risk assessments)