Holy Cross Hospital

Security Policy

Target Group: All Caregivers, Visitors and Contractors	Version: 14	Issue Date: 18 September 2025
Approved by: Leadership Team 18 September 2025	Date Last Approved/Reviewed: August 2023	Effective Date: September 2025- August 2028

Printed copies are for reference only. Please refer to the electronic copy for the latest Version

Holy Cross Hospital

Contents

1. Introduction

Holy Cross Hospital is committed to safeguarding patients, Caregivers, and visitors from security risks within its premises. This policy outlines the measures in place to prevent unauthorised access, theft, aggression, and to ensure the safe management of keys, valuables, and property.

This policy will be reviewed every three years, or sooner if required due to legislative or regulatory changes, organisational needs, or following a significant security incident.

The Director of Operations is responsible for ensuring the policy remains current, compliant, and reflective of best practice.

2. Purpose

The purpose of this policy is to establish a robust and consistent approach to security across all areas of Holy Cross Hospital. It sets out clear expectations and responsibilities for maintaining the safety and security of patients, Caregivers, visitors, and property.

This policy aims to:

- Safeguard individuals from harm, violence, theft, or loss while on hospital premises.
- Prevent unauthorised access to the hospital, its departments, and sensitive areas through effective access control.
- Protect confidential information, valuable assets, and hospital property via secure storage and procedures.
- Define clear protocols for managing keys, responding to security breaches, handling lost property, and conducting departmental close-downs.
- Promote a security-conscious culture where all Caregivers are responsible for upholding and reporting security concerns.
- Ensure security arrangements support the delivery of high-quality, safe, and well-led care in line with legal and regulatory requirements.
- Minimise disruption to hospital services caused by preventable security incidents or breaches.

3. Objectives of this Policy or Procedure

This policy supports the following objectives:

- Prevent unauthorised access to hospital premises.
- Protect Caregivers, patients, and visitors from harm.
- Prevent theft, fraud, or misuse of property.
- Support a safe and welcoming environment.
- Ensure clear roles and responsibilities in managing security risks.

- Set expectations for Caregiver conduct regarding security.

4. Policy Statement

Holy Cross Hospital is committed to ensuring the safety, security, and wellbeing of all individuals within its premises. A secure environment is essential for delivering high-quality care and protecting people, property, and sensitive information.

This policy establishes the framework for preventing and managing security risks, including unauthorised access, theft, fraud, violence, and vandalism. Security measures apply to both physical areas (buildings and grounds) and the safeguarding of data, assets, and personal belongings.

The hospital promotes a culture of vigilance, accountability, and shared responsibility. All Caregivers and authorised personnel are expected to comply with established security procedures, challenge inappropriate or suspicious behaviour, and report concerns promptly.

Security is integrated into operational planning, Caregiver training, and emergency preparedness. Through clear procedures, robust monitoring, and continual review, this policy supports proactive risk management and ensures Holy Cross Hospital remains a safe and trusted environment for care delivery.

5. Scope

This policy applies to:

- All Caregivers employed by or working on behalf of the hospital.
- All contractors, volunteers, and visitors.
- All physical areas of the hospital and its grounds.
- All assets, including information and equipment.

6. Responsibilities

Security is a shared responsibility across all levels of the organisation. Each individual has a role to play in maintaining a secure and safe environment. The following outlines key responsibilities:

Chief Executive

- Holds overall accountability for ensuring the hospital provides a secure environment for patients, Caregivers, visitors, and contractors.

Director of Operations

- Policy owner responsible for the development, implementation, and review of the Security Policy.
- Leads on security audits, investigations into breaches, and ensures policy compliance across the organisation.

Facilities and Housekeeping Lead

- Carries out six-monthly key audits to ensure accountability and compliance.
- Issues keys to authorised personnel and ensure all issued keys are accurately recorded and tracked.
- Supports the maintenance of secure access to hospital areas and report any breaches or concerns.

Health and Safety Committee

- Monitors the effectiveness of this policy via regular review of incident reports and audit findings.
- Recommends improvements to policy or procedure based on evidence or trends.
- Supports cross-departmental learning from incidents or breaches.

Reception Team

- First point of contact for visitor access and responsible for issuing and logging identification badges.
- Maintains lost and found records and logs all security-related reports and incidents securely.
- Ensures departmental keys are managed in accordance with the key control protocol.

Departmental Managers / Team Leaders

- Responsible for implementing this policy within their area of responsibility and ensuring that departmental close-down procedures (Appendix 3) are followed.
- Maintain departmental key registers and complete scheduled audits of key cabinets and storage.
- Ensure that all Caregivers within their teams are trained on security procedures and understand expectations.
- Lead internal investigations into any security breaches or missing property, escalating serious matters to the Director of Operations.

Nurse-in-Charge (Bleep Holder)

- Maintains oversight of security during clinical shifts, including safe access to the premises outside of Reception hours.
- Responds to security incidents, including activation of the panic alarm system. (Appendix 2)
- Ensures master key handovers are properly recorded and managed.

All Caregivers

- Must comply with all elements of this policy, including wearing ID badges, securing personal and hospital property, and challenging unauthorised persons where safe to do so.
- Responsible for ensuring doors are not wedged open or left insecure.
- Report any suspicious activity, lost property, missing keys, or breaches of procedure to their line manager or Nurse-in-Charge without delay.
- Follow all departmental close-down (Appendix 3) and key management procedures.
- Maintain confidentiality and refrain from discussing any element of the hospital's security arrangements with unauthorised individuals.

Maintenance Team

- Responsible for securing departmental areas in line with close-down checklists (App. 3).
- Conduct regular checks on lighting, entry points, and outdoor areas to identify and report risks such as open windows, faulty locks, or unsecured waste.
- Ensure secure storage and handling of tools and equipment.

7. Definitions

Security Breach
An incident involving unauthorised access, theft, damage to property, loss of keys or door codes, or failure to follow security procedures that compromises the safety or integrity of the hospital environment.

Key Register
A controlled record used to document the issue, return, and audit of physical keys across all departments. It includes the names of key holders and associated access permissions.

Door Code
A security code used on keypad-entry systems to control access to restricted areas of the hospital. These codes are confidential and are only issued to authorised Caregivers.

Visitor Management System
A digital platform used to log the arrival and departure of all visitors and contractors to the hospital. It supports security monitoring, traceability, and the issuing of visitor identification badges.

Panic Alarm
A fixed alarm system used to summon immediate assistance in situations where a Caregiver is experiencing aggression, violence, or another serious threat. Activation triggers a predefined emergency response.

Master Key
A high-level access key that opens multiple or all locked areas within the hospital. Master keys are tightly controlled and held only by authorised Senior Caregivers, including the Nurse-in-Charge.

Close-down Procedure
A routine process undertaken by designated Caregivers to ensure departments are secured at

the end of the working day. This includes locking doors, switching off equipment, and securing sensitive information or valuables. See Appendix 3 for close-down procedures

CCTV (Closed Circuit Television)
Surveillance cameras installed in key access points and sensitive areas to monitor, deter, and record suspicious or unauthorised activity. Used in accordance with data protection legislation.

Audit
A formal review or inspection process used to evaluate compliance with defined security procedures, such as key management, door code changes, or incident logging. Audits may be scheduled or unannounced.

Unauthorised Access
Entry into a restricted area by an individual who does not have the appropriate permissions, identification, or justification. This includes both external intruders and internal personnel breaching access protocols.

8. Policy or Procedure Implementation

8.1 External Door Security

All external doors, except the automatic front entrance, are designed to lock automatically when closed. These doors must remain locked at all times unless actively in use. The front entrance remains in automatic mode during Reception hours to support accessibility. Outside of these times, access is managed via the intercom and approved by the Nurse-in-Charge.

Two rear hospital doors operate via keypads. Codes are distributed to authorised Caregivers only, are updated regularly, and must never be shared. Caregivers should generally use these designated entrances.

All external doors (excluding the automatic front door and designated service entrances) are alarmed. Door alarms trigger alerts to designated pagers when activated and may be manually engaged by the Nurse-in-Charge.

8.2 CCTV Monitoring and Door Security Compliance

Closed Circuit Television (CCTV) is installed at the Caregivers' Entrance to support site security and monitor compliance with door control protocols.

The CCTV system is used solely for safety, security, and investigation purposes in line with the Data Protection Act 2018 and UK GDPR. Holy Cross Hospital is the Data Controller for all recordings.

- Privacy Notices and Signage: Clear signage is displayed at all monitored areas to inform patients, visitors, and Caregivers that CCTV is in operation, the purpose of monitoring, and how further information can be obtained.
- Access to Recordings: Access is restricted to authorised personnel only. Requests for disclosure to third parties (e.g., the police) must be formally logged and approved by the Director of Operations or Data Protection Officer.

- Retention of Recordings: CCTV footage is retained for a maximum of 30 days unless required as evidence in an ongoing investigation or legal matter.
- Data Subject Rights: Individuals may request access to CCTV recordings in which they appear, in accordance with the hospital's Subject Access Request procedure.

Caregivers are reminded that all external doors must remain closed and locked unless actively in use. Under no circumstances should any door be propped or wedged open and left unattended.

Where CCTV or incident reports show that a Caregiver has failed to secure an external door—either by deliberately propping it open or neglecting to ensure it has closed properly—this will be treated as a breach of the Security Policy. Depending on the circumstances, this may lead to formal disciplinary action in line with the organisation's Disciplinary Policy

8.3 Door and Key Safe Code Management

To maintain site security and prevent unauthorised access, all door codes (including those for Caregivers entrances, service doors, and restricted access areas) must be changed at least every six months. This process is overseen by the Maintenance Department, with oversight from the Director of Operations.

The following principles apply:

Frequency: All door codes must be updated on a six-monthly basis, or sooner if there is reason to believe that a code has been compromised (e.g. following Caregivers turnover, a security breach, or a lost access record).

Authorised Access: New codes are to be shared only with authorised Caregivers who require access as part of their role.

Secure Communication: Distribution of codes must be carried out in a secure and traceable manner. Codes must not be shared verbally in open areas or written in visible or unsecured locations.

Code Confidentiality: Caregivers must not disclose door codes to unauthorised persons, including visitors, contractors, or colleagues without access rights.

Monitoring and Audit: The Maintenance Department will maintain a record of code changes and distribution logs. Spot checks may be carried out to ensure compliance with secure handling.

Failure to comply with door code confidentiality requirements may result in disciplinary action, as it constitutes a breach of this policy and could place patients, Caregivers, and property at risk.

8.4 Caregivers Security Guidelines

All Caregivers play a critical role in maintaining a secure and safe environment. The following guidelines outline expected conduct in relation to security practices on-site:

Maintain Door Security: External doors must never be propped or wedged open, except for brief periods when necessary for manual handling—and only while under active supervision.

Use Designated Entrances: Entry and exit must be via the authorised Caregivers' or Stores Entrance, both of which are access-controlled.

Protect Access Credentials: Keypad codes are confidential and must not be disclosed to any unauthorised individuals.

Remain Vigilant: Any suspicious behaviour, persons, or activity must be reported immediately to the Nurse-in-Charge or a senior manager.

Wear Identification: Hospital-issued ID badges must be visibly worn at all times while on duty.

Challenge Politely: Caregivers are expected to respectfully challenge individuals not displaying ID to confirm their authorisation to be on-site.

Limit Personal Valuables: Only essential personal items should be brought on-site. The hospital does not accept liability for loss or theft of personal property.

Secure Personal Belongings: All personal items must be stored in lockers (or locked drawers for office-based Caregivers).

Preserve Security Confidentiality: Details of the hospital's security procedures must not be discussed with external parties unless explicitly authorised by a senior manager.

Adhere to Close-Down Protocols: Departments must follow designated close-down procedures (App. 3) in full. Where this is not possible, the Nurse-in-Charge must be informed without delay.

8.5 Key Security

The Estates and Facilities Team holds overarching responsibility for the management and security of keys across the hospital. Keys are only issued where there is a defined operational need, and all issued keys must be logged in the official key register. Individuals who are issued keys are personally accountable for their safekeeping and appropriate use.

Keys must never be labelled with the name of a room, department, or function. Labelling should be limited to the hook or case reference number to minimise security risks if misplaced.

All senior nursing Caregivers, must be familiar with the hospital's key storage and access procedures to provide assistance to emergency services personnel if required.

Key Audits

Main Key Cupboards: Audited at least every six months by the Facilities and Housekeeping Lead (FHL).

Departmental Key Cabinets: Audited annually by the relevant Department Manager, or nominated person.

Audit Reporting: All audit findings are submitted to the Director of Operations for review and action where necessary.

8.6 Master Key Handover Procedure

The Nurse-in-Charge is responsible for the secure handover of the master key set at each shift change.

A secondary set of master keys is securely stored in a coded key safe, located in the corridor near the medical archive cupboard and accessible to authorised Reception personnel.

The Housekeeping Team has access to sub-master keys to facilitate essential cleaning tasks outside of standard operational hours. These are stored in a secure key safe located in the Laundry Lobby.

Any loss or suspected misplacement of keys must be reported immediately to a manager, senior nurse, or member of the Estates and Facilities Team. An incident form must be completed without delay. Under no circumstances should keys be issued or loaned to individuals without proper authorisation.

8.7 Lost and Found Procedure

Caregivers must report lost items to Reception with details including owner name, item description, and where it was lost. Found items should be handed to a Senior Caregivers or Reception (if of significant or unknown value). Items of minor value may be kept in the department for 3 months before disposal.

Items of value will be stored securely for 6 months while efforts are made to trace the owner. If claimed, a receipt must be issued. Uncollected patient or Caregivers property will be treated as unclaimed if not retrieved following written notification.

8.8 Panic Alarm Procedure (Reception)

The panic button is for use only during escalated conflict situations. Alerts are sent to designated bleep holders, who must assess the scene discreetly from the link corridor. If escalation continues, they must call emergency services on 999 with full details. (Appendix 2)

8.9 Visitor Management System

The hospital operates a digital visitor management system to monitor and control access to the premises, ensuring the safety and security of patients, Caregivers, and property. All visitors must sign in and out using this system upon arrival and departure.

Digital Sign-In Points

There are two dedicated visitor registration points:

Main Reception: This is the primary sign-in point for all general visitors, including families, external professionals, and suppliers.

St Hugh's Entrance: A secondary digital screen is provided for contractors and other service personnel entering via this access point.

Each visitor is required to provide their name, the purpose of their visit, and the department or person they are attending. Upon successful registration, a visitor badge will be issued.

Identification Badges

All visitors must wear their visitor badge visibly at all times while on site. Badges help Caregivers and Caregivers quickly identify authorised individuals and ensure that all persons present have signed in appropriately.

Challenging Unbadged Individuals

Caregivers are expected to challenge, in a courteous and professional manner, any individual seen on the premises without an ID badge. If there is any uncertainty regarding a person's authorisation, the

matter must be reported immediately to Reception or the Nurse-in-Charge. This expectation forms part of the hospital's shared responsibility for maintaining a secure environment.

8.10 Training & Awareness

- All new Caregivers, contractors, and volunteers receive security awareness training at induction which is covered in the Directors of Operation's session.
- Annual refresher training is provided for all staff, with content tailored to recent audit findings and incidents.
- Departmental staff are trained in their local close-down procedures and reminded regularly of their responsibilities for securing windows, doors, keys, and confidential information.
- Bleep Holders, Reception staff, and key-holders receive additional role-specific training (e.g., nightly checks, key register completion, panic alarm use).
- Awareness is reinforced through signage, bulletins, team briefings, and audit feedback.
- Training compliance is monitored via the Learning & Development system and reported to the Health & Safety Committee.

9. Regulatory Requirements/ References

This policy aligns with the following legal and regulatory frameworks, best practice standards, and internal governance requirements:

Statutory and Regulatory Frameworks

- Health and Safety at Work etc. Act 1974 – Duty to ensure the health, safety, and welfare of employees and others on site.
- Management of Health and Safety at Work Regulations 1999 – Requirement to assess risks and implement control measures.
- The Care Quality Commission (CQC) Fundamental Standards, especially:
    - Regulation 12: Safe care and treatment – Including premises safety and protection from harm.
    - Regulation 15: Premises and equipment – Ensuring the environment is secure and well maintained.
    - Regulation 17: Good governance – Including maintaining robust systems to protect people from harm.
- The Health and Social Care Act 2008 (Regulated Activities) Regulations 2014
- The Equality Act 2010 – Especially in relation to safeguarding and accessibility in visitor management.
- The Data Protection Act 2018 / UK GDPR – Relevant to CCTV use, visitor information systems, and lost property data handling.

National and Professional Guidance

- NHS England Violence Prevention and Reduction Standards (2021) – Applicable to managing abuse, aggression, and intruders.
- HTM 07-01: Safe Management of Healthcare Waste – Where waste-related fire risk or security risks exist (e.g. arson).

10. Evaluation Measures

- Annual security policy audit by Director of Operations (Appendix 4)
- Incident trend analysis by the Health and Safety Committee
- Spot-checks of key logs and access points
- Evaluation of panic alarm use and response times
- Lost property and theft reports logged and reviewed quarterly

11. Related Documents

This policy should be read in conjunction with the following documents, which provide further guidance and specific procedures relevant to maintaining a secure environment:

- Management of Aggression and Violence Policy
- Disciplinary Policy
- Caregivers Handbook
- Controlled Drugs Operational Standards (for Controlled drug security)
- Operational Policy for Medical Gas
- Patients' Money and Property Policy
- Information Management Policy
- Private Transactions and Acceptance of Gifts Policy
- Donations and Charitable Gifts Policy
- Visiting Patients Policy
- Safeguarding Policy
- Business Continuity Plan
- Security Risk Assessment (Appendix 5)

12. Appendices

Appendix 1 – Equality Impact Assessment (EIA) Tool

To be considered and where judged appropriate, completed and attached to any policy document when submitted to the appropriate committee for consideration and approval.

Policy Title	Security Policy

		Yes/No	Comments
	Does the policy/guidance affect one group less or more favourably than another on the basis of:		
	Race	No	Signage, ID checks, and visitor management apply equally to all. Translation support or interpreters can be made available where language barriers may exist.
	Gender reassignment	No	Security measures apply consistently regardless of gender. Caregivers and visitors are not treated differently. Facilities are gender-neutral where appropriate.(eg Toilets)
	Marriage & civil partnership	No	No impact identified. The policy makes no distinction based on marital or partnership status, and respectful treatment is expected of all individuals.
	Pregnancy & maternity	No	No negative impact anticipated. Security measures (e.g., access control, CCTV) do not restrict access for pregnant staff, patients, or visitors.
	Ethnic origins (including gypsies and travelers)	No	No adverse impact anticipated. Security procedures apply equally to all individuals, with respect for cultural needs where relevant.
	Nationality	No	No negative impact identified. Visitor management and ID checks are applied consistently, and support can be provided if documentation is unclear or language support is required.

	Sex	No	Policy applies equally to male and female individuals; no differential impact identified.
	Culture	No	Security checks and visitor protocols are applied fairly across cultural groups, with sensitivity to cultural practices when appropriate.
	Religion or belief	No	No discriminatory impact identified.
	Sexual orientation	No	No impact identified. The policy is neutral in respect of sexual orientation and applies equally to all Caregivers, patients, and visitors.
	Age	No	Younger or older visitors may require additional support with digital visitor management (e.g., touchscreens). Reception will provide assistance as needed.
	Disability- both mental and physical impairments	No	CCTV and door controls do not disadvantage people with disabilities. Visitor management systems are accessible, and adjustments (e.g., wheelchair access at entrances, support with forms) are provided on request.
2.	Is there any evidence that some groups are affected differently?	No	
3.	Is the impact of the policy/guidance likely to be negative?	No	
4.	If so can the impact be avoided?	N/A	
5.	What alternatives are there to achieving the policy/guidance without the impact?	No	
6. >--	Can we reduce the impact by taking different action?	N/A	
7.	If you have identified potential discrimination, are any exceptions valid, legal and/or justifiable?	NO	

Appendix 2- Panic Alarm Response Procedure

Purpose

To outline the appropriate and immediate actions to be taken when a panic alarm is activated within the hospital, ensuring a coordinated, safe, and effective response to potential threats or violent incidents.

Procedure

Activation of Panic Alarm

- The panic alarm system may be activated from Reception
- Activation should occur only in situations where a Caregiver feels threatened, unsafe, or is experiencing a conflict situation that cannot be safely managed without assistance.
- Immediate Response
- The panic alarm will send a signal to designated bleep holders pagers across the hospital.
- The primary responder must proceed immediately—but discreetly—to the scene (e.g., the upper link corridor window above Reception).
- If it is safe, the responder should observe from a distance to assess the situation without escalating it.

Assessment and Communication

- The responder should attempt to discreetly assess:
- Whether the situation appears calm, escalating, or dangerous.
- Whether immediate support or police presence is required.
- If the situation is deemed to require police attendance, the responder must dial 999 and clearly state:
    - The hospital name and address.
    - Nature of the incident.
    - Exact location within the hospital.

Post-Incident Actions

Once the situation has been resolved, the Nurse-in-Charge must:

- Ensure the wellbeing of the Caregivers(s) involved.
- Complete an incident report form with details of the event, response, and outcome.
- Notify the Director of Operations and Safeguarding Lead (if applicable).
- Record the incident on the central incident log for review by the Health and Safety Committee.

Review and Follow-Up

- All panic alarm activations are to be reviewed at the next Health and Safety Committee meeting.
- Follow-up actions may include:
- Additional support or supervision for the Caregivers involved.

- Conflict resolution or de-escalation training.
- Adjustments to physical security arrangements, staffing, or layout.

Training and Awareness

Reception Caregivers, bleep holders, and Nurse-in-Charge, must receive training on the location, use, and response expectations of the panic alarm system.

Regular drills or refresher sessions should be conducted at least annually.

Appendix 3 – Departmental Close-Down Procedures

To ensure the security and safety of hospital premises, the following close-down procedures must be completed by the last Caregivers on duty in each area. Where a procedure cannot be completed, the Nurse-in-Charge must be informed immediately.

Catering Department

The catering department, including store rooms, fridges, and freezers, is in daily use between approximately 6:30am and 8:00pm.

Caregivers' Dining Room (in use overnight):

- Check that supplies of milk, tea, and coffee are available for night Caregivers.
- Secure the serving hatch.
- Close the patio doors to the decking area.

Overnight Close-Down (Kitchen and Store Rooms):

- Ensure all windows are closed.
- Ensure all water taps are turned off.
- Switch off all gas and electrical appliances correctly.
- Empty all bins and remove rubbish.
- Lock all inner doors: stock room, equipment store, walk-in fridge, and freezer.
- Lock the back door and the door to the Caregivers' dining room.
- Switch off all lights.
- Exit via the main trolley entrance and deposit keys in the key safe.

Stores Close-Down Procedure

- Close and lock all windows.
- Turn off all taps.
- Empty all bins.
- Lock the main door from the inside.
- Secure keys in the stores key safe.

Laundry Department

In operation daily between 7:00am and 4:00pm (with reduced hours on weekends and bank holidays).

Overnight Close-Down:

- Ensure all windows are closed.
- Turn off all water taps.
- Switch off all gas and electrical appliances.
- Empty all bins and remove rubbish.
- Ensure the rear laundry fire door is closed and secured.
- Lock all inner doors: stock room and office.
- Switch off all lights.
- Lock the inner laundry room door.
- Leave the outer laundry door unlocked (to allow Caregivers to drop off soiled linen after hours).
- Place keys in the laundry key safe.

Maintenance Department (Workshop)

- Notify Reception that the department is closing.
- Close all windows.
- Turn off all electrical equipment.
- Lock the key case.
- Turn off all lights.
- Secure the main workshop door.

Reception Close-Down & End of Business Procedure

At the end of each working day, the Reception area and associated facilities must be securely closed down before staff leave the premises.

Key tasks include:

- Completing end-of-day financial and reporting tasks.
- Printing and preparing the following day's appointments and diaries.
- Ensuring all forms, rotas, and front desk materials are in place.
- Securing cash, valuables, keys, and sensitive information in accordance with the Key Management and Finance Procedures.
- Locking doors, windows, and cupboards, and ensuring all equipment is appropriately shut down or placed on charge.
- Securing the hydrotherapy pool, St Hugh's access points, and other linked areas as required.
- Disposing of confidential waste securely.
- Completing final security checks, including setting alarms, locking doors, and switching phone systems to night service.

For the detailed step-by-step process**,** including system access, financial tasks, and specific key allocations, please refer to the Reception Operational Procedures**.**

Offices (General Use)

- Lock all drawers, filing cabinets, and cupboards.
- Switch off all electrical equipment.
- Close all windows.
- Turn off all lights.
- Lock the office door.

St Hugh's Office Area

- Lock all drawers, filing cabinets, and cupboards.
- Leave desks tidy.
- Switch off all electrical equipment.
- Check the kitchen area downstairs.
- Close all windows.
- Turn off all lights (note: one PIR light may remain on).
- Lock both the upstairs and downstairs doors.

Patients' Activities and Therapy Areas

Includes the dayroom and office, occupational therapy kitchen, St Anne's, physiotherapy inpatient/outpatient gyms and offices, and hydrotherapy suite:

- Turn off all electrical equipment.
- Close all windows.
- Turn off all lights.
- Lock all doors.

St Hugh's Training Area

(Responsibility lies with the person booking the space)

- Turn off all electrical equipment, including the coffee machine, projector, and screen.
- Store laptop and projector securely if used.
- Close all windows.
- Switch off all lights.
- Lock all external doors and return keys to the key safe.

Night Duty Bleep Holder Security Check Procedure

The Bleep Holder is responsible for completing security checks each night, addressing any immediate issues, and reporting unresolved matters to the Nurse-in-Charge and Director of Operations.

General Checks

- Conduct a walk-round of all patient areas, activity spaces, and communal rooms.
- Ensure all external doors are secure and not wedged open.
- Confirm that all emergency exits are closed but remain operational in case of evacuation.

Windows

- Check and close any open windows in:
- Changing rooms
- Patients' activities and therapy areas
- Offices and non-clinical spaces not in use overnight
- Report any windows that cannot be closed to Maintenance via the on-call rota.

Incident Reporting

Any security breaches, suspicious activity, or hazards identified must be reported using the Incident Reporting System.

If urgent (e.g., broken locks, intruder concerns), escalate to the on-call maintenance officer and/ or on call senior manager and/or emergency services as appropriate.

Handover

Provide a security update at morning handover, highlighting any issues identified and actions taken.

Appendix 4- Security Audit Tool

Audit Title: Security Policy Compliance Audit
Audit Lead: [Name/Role]
Audit Period: From [DD/MM/YYYY] to [DD/MM/YYYY]
Departments Audited: [List]
Date Completed: [DD/MM/YYYY]

Item	Yes	No	N/A	Comments / Evidence
Are all external doors secure and fitted with functioning locks/alarms?	☐	☐	☐	
Are all emergency exits closed, unobstructed, and operational for evacuation?	☐	☐	☐	
Are windows in non-clinical areas (offices, changing rooms, activity rooms) closed and secure?	☐	☐	☐	
Is CCTV signage displayed in all monitored areas?	☐	☐	☐	
Is CCTV footage being retained in line with policy (e.g., 30 days)?	☐	☐	☐	
Are visitor management systems working (sign-in, ID badge issue)?	☐	☐	☐	
Are unbadged visitors challenged appropriately?	☐	☐	☐	

Are external areas (car parks, footpaths) well-lit and functional?	☐	☐	☐	
Are keypad/fob systems operational and codes/cards up to date?	☐	☐	☐	
Are intruder/fire alarm panels checked and faults cleared?	☐	☐	☐	
Is there a log of who holds keys or fobs?	☐	☐	☐	
Are high-risk assets (medication, IT, tools) kept locked away?	☐	☐	☐	
Are restricted areas clearly marked with signage?	☐	☐	☐	
Is there a process for staff to report security concerns or breaches?	☐	☐	☐	

Appendix 5– Security Risk Assessment and Mitigation Measures

This appendix outlines key security-related risks within the hospital environment and the control measures in place to mitigate them.

Risk	Control Measures
Unauthorised entry – potential harm to patients or visitors	- Keep all external doors secured when not in active use. - Limit access to a single monitored entry point. - Ensure all individuals on-site wear a uniform or ID badge. - Encourage Caregivers to respectfully challenge unknown individuals. - Authorise managers to ask unauthorised persons to leave.
Authorised entry – potential harm from permitted individuals	- Clearly communicate and enforce visiting arrangements. - Ensure all visitors are signed in and issued with badges. - Empower managers to respond to abusive, threatening, or violent behaviour, including asking individuals to leave or contacting police. - Conduct risk assessments for individuals whose presence raises concern.
Violence or abuse towards caregivers	- Monitor individuals for early signs of agitation or escalation. - Provide training in de-escalation and conflict management. - Support senior Caregivers in making timely decisions. - Ensure external areas (e.g. car parks, footpaths) are well-lit and safe.
Theft within the building	- Secure high-risk assets and conduct regular inventory checks. - Maintain a locked-door policy for external and designated internal areas.

	- Routinely check rooms not in regular use. - Store cash, valuables, and medications in locked safes or drawers. - Follow controlled procedures for receiving and storing supplies. - Provide patients with individual lockable storage.
Theft or damage outside the building	- Ensure adequate lighting in outdoor areas and car parks. - Conduct regular checks of external zones. - Encourage prompt reporting of suspicious behaviour. - Collaborate with neighbours and local police to monitor activity.
Arson	- Apply all external property security measures. - Keep waste areas clean and bins securely locked. - Include external ignition risks in fire risk assessments.
Fraud	- Follow robust procurement procedures. - Adhere to internal financial controls as defined by auditors. - Maintain strict processes for handling salaries, petty cash, and financial transactions.