



Royal Cornwall Hospitals
NHS Trust

Security Policy

V7.0

December 2025

Summary

Manager's Responsibility

- All managers are responsible for the implementation of day-to-day security arrangements within their locations, services and departments. All managers have a responsibility to ensure that all staff are aware of the Trust Security Policy, standards, procedures and guidelines.
- Ensure that Security risks are regularly assessed and appropriate controls are implemented. Action plans must be drawn up in response to identified risks.
- Identify training needs in relation to the personal security of staff and enable staff to undertake such training.
- Ensure adequate arrangements exist to maintain the security of staff, patients, visitors, premises and equipment under their control.
- Ensure that preventative measures are taken to secure valuable and attractive items and an accurate inventory of equipment and its whereabouts is maintained.
- Ensure that all data and records are held securely. Computer data must be adequately protected and written records must be locked away, in line with the requirement of the Trust's [Information Security Policy](#).
- Ensure that there are written procedures to ensure the physical security of all doors and windows is adequate when premises are vacated.

Role of Individual Staff / Volunteers / Contractors

- Employees must co-operate with management to achieve the aims of this security policy.
- It is RCHT policy for all its employees, including volunteers and contractors to be issued with a photo identity card. All groups are required to wear this ID at all times when on duty, even if they also wear easily recognised uniforms or name badges.
- Where staff become aware of actual or potential breaches of security, all such incidents must be reported via the Datix system, in accordance with the Trust's [Patient Safety Incident Response Policy](#).
- It is an offence to remove (or borrow) any RCHT property without agreement from their Departmental Manager. Failure to do so could result in disciplinary action/and or criminal proceedings being taken.
- Staff should be aware of any local security policy relevant to each of the RCHT sites they may operate from.

Table of Contents

Summary	2
1. Introduction	5
2. Purpose of this Policy.....	5
3. Scope.....	5
4. Definitions / Glossary.....	5
5. Ownership and Responsibilities	6
5.1. The Security Management Director (SMD)	6
5.2. The Non-Executive Directors (NEDs).....	6
5.3. The Trust Security Lead (LSMS)	6
5.4. Role of Managers	7
5.5. Role of Individual Staff / Volunteers / Contractors	7
6. Standards and Practice.....	8
6.1. Risk Management.....	8
6.2. Fraud	8
6.3. Reporting Of Crime and Security Incidents	9
6.4. Working in Partnership with the Police	9
6.5. Sanctions	9
6.6. Protection of Critical Assets	10
6.7. Site Security.....	10
6.8. Building Security.....	10
6.9. Personal Security of Staff.....	10
6.10. Asset Management.....	11
6.11. Security Marking of Valuable Equipment.....	11
6.12. Recovery of Losses	11
6.13. Identification of Personnel	11
6.14. Conflict Resolution Training	12
6.15. Security of Computerised Information	12
6.16. Security of Health Records.....	12
6.17. Closed Circuit Television (CCTV)	12
6.18. Purchase of Security Systems	12
6.19. Bomb Threat/Suspect Packages.....	12
6.20. Lockdown.....	13
6.21. Escalation of Security Incident	13
6.22. Firearm or Weapons Attack.....	13

6.23. Managing Security Alerts	14
6.24. Training	14
7. Dissemination and Implementation	14
8. Monitoring compliance and effectiveness	14
9. Updating and Review	15
10. Equality and Diversity	15
Appendix 1. Governance Information	16
Appendix 3. Guide to Good Practice for the Security of Premises	22
Appendix 4. Security Identity Badge Protocol	24
Appendix 5. Procedure for Reporting Criminal and Security Incidents	29
Appendix 6. Procedure for Staff Receiving a Telephone Bomb Threat or finding a Suspicious or Unattended Package	31

Data Protection Act 2018 (UK General Data Protection Regulation – GDPR) Legislation.

The Trust has a duty under the Data Protection Act 2018 and UK General Data Protection Regulations 2016/679 to ensure that there is a valid legal basis to process personal and sensitive data. The legal basis for processing must be identified and documented before the processing begins. In many cases we may need consent; this must be explicit, informed, and documented. We cannot rely on opt out, it must be opt in.

Data Protection Act 2018 and UK General Data Protection Regulations 2016/679 is applicable to all staff; this includes those working as contractors and providers of services.

For more information about your obligations under the Data Protection Act 2018 and UK General Data Protection Regulations 2016/679 please see the Information Use Framework Policy or contact the Information Governance Team.

Royal Cornwall Hospital Trust rch-tr.infogov@nhs.net

1. Introduction

- 1.1. The Board of the Royal Cornwall Hospitals NHS Trust are aware of their legal responsibility to provide a safe and secure environment for patients, staff and visitors whilst on Trust property. The protection of Trust resources is considered to be the responsibility of all who work within the Trust's hospitals and other premises.
- 1.2. Security is the responsibility of all staff in not only safeguarding their own wellbeing, but that of patients and visitors. The safeguarding of the Trust's property and resources against crime is of paramount importance and the primary objectives are:
 - 1.2.1. Personal safety of patients, staff, visitors and residents at all times.
 - 1.2.2. Protect the assets of the Trust against fraud, dishonesty, damage and litigation.
 - 1.2.3. Reduce crime on the hospital's sites and address any other security malpractice that impinges on the management of health care delivery.
 - 1.2.4. To work with partnership agencies to contribute to a safer community.
- 1.3. This version supersedes any previous versions of this document.

2. Purpose of this Policy

- 2.1. All NHS organisations are required to provide a clearly defined and robust security policy that reflects the individual nature and character of the organisation.
- 2.2. The purpose of the Security Policy is to support the Royal Cornwall Hospitals NHS Trust in the delivery of high-quality clinical services, through the provision of a secure environment.

3. Scope

- 3.1. This policy covers all assets of the Trust together with the management and reporting function necessary to implement the policy.
- 3.2. Standards, procedures and guidelines, designed to minimise the effects of potential threats are detailed in section 11 (Standards and Practice) of this policy.
- 3.3. Standards, procedures and guidelines will be reviewed and issued where and when necessary. They will be deemed to form part of this policy and all staff should comply with them. Copies will be made available to all staff.

4. Definitions / Glossary

- NHS England: NHS England leads on work to identify and tackle crime across the National Health Service.

- SMD: Security Management Director.
- NED: Non- Executive Director.
- LSMS: Trust Security Lead (LSMS) – Local Security Management Specialist.
- Official Visitors: Those present for half a day or more, or who may be left unattended on Trust premises.

5. Ownership and Responsibilities

Overall responsibility for security within the Royal Cornwall Hospitals NHS Trust rests with the Chief Executive. However, operational responsibility is delegated to an Executive Board member in the role of Security Management Director.

5.1. The Security Management Director (SMD)

An Executive member of the Trust board will be responsible for adopting the role of the nominated Security Management Director under the NHS Standard Contract as published by NHS England. The Director has board level responsibility for Security Management within the Trust and to support the Local Security Management Specialist in their role so they can fulfil their duties and statutory requirements.

5.2. The Non-Executive Directors (NEDs)

To promote security management work from the non-executive function at board level, to challenge, scrutinise and ensure accountability in respect of security management work.

5.3. The Trust Security Lead (LSMS)

- 5.3.1. Is responsible to the Security Management Director to take forward security management work locally, in line with national standards; to undertake the duties of an LSMS in accordance with the NHS Standard Contract as published by NHS England to health bodies on measures to tackle violence and general security management measures, and any subsequent advice or guidance issued by NHS England.
- 5.3.2. Support the day-to-day work of the Trust in line with the VPR strategy and in relation to tackling violence against staff and professionals in accordance with NHS England's national framework and guidance.
- 5.3.3. Ensure that appropriate steps are taken to create a pro-security culture within the Trust so that staff and patients accept responsibility for this issue and ensure that where security incidents/breaches occur that they are detected and reported.
- 5.3.4. Ensure that appropriate security incidents/breaches are publicised appropriately in accordance with guidelines issued by NHS England to allow the development of preventative measures.

- 5.3.5. Monitor the investigation and prosecution of incidents, assisting the Police when necessary.
- 5.3.6. Work towards applying a range of sanctions against those responsible for security incidents/breaches, are progressed accordingly.
- 5.3.7. Ensure that, where appropriate, redress is sought from those who commit security incidents/breaches and where a loss of resources is incurred.
- 5.3.8. To provide a written report, at least once in every financial year, summarising the Trust Security Lead (LSMS) work for that year, and to submit a copy to NHS England.

5.4. Role of Managers

- 5.4.1. All managers are responsible for the implementation of day-to-day security arrangements within their locations, services and departments. All managers have a responsibility to ensure that all staff are aware of the Trust Security Policy, standards, procedures and guidelines.
- 5.4.2. Ensure that Security risks are regularly assessed and appropriate controls are implemented. Action plans must be drawn up in response to identified risks.
- 5.4.3. Identify training needs in relation to the personal security of staff and enable staff to undertake such training.
- 5.4.4. Ensure adequate arrangements exist to maintain the security of staff, patients, visitors, premises and equipment under their control.
- 5.4.5. Ensure that preventative measures are taken to secure valuable and attractive items and an accurate inventory of equipment and its whereabouts is maintained.
- 5.4.6. Ensure that all data and records are held securely. Computer data must be adequately protected and written records must be locked away, in line with the requirement of the Trust's [Information Security Policy](#)¹.
- 5.4.7. Ensure that there are written procedures to ensure the physical security of all doors and windows is adequate when premises are vacated.

5.5. Role of Individual Staff / Volunteers / Contractors

- 5.5.1. Employees must co-operate with management to achieve the aims of this security policy and local measures implemented.
- 5.5.2. It is RCHT policy for all its employees, including volunteers and contractors to be issued with a photo identity card. All groups are required to wear this ID at all times when on duty, even if they also wear easily recognised uniforms or other name badges.

- 5.5.3. Where staff become aware of actual or potential breaches of security, all such incidents must be reported in accordance with the Trust incident reporting policy, via the Datix system.
- 5.5.4. It is an offence to remove (or borrow) any RCHT property without agreement from their Departmental manager. Failure to do so could result in disciplinary action/and or criminal proceedings being taken.
- 5.5.5. Staff should be aware of any local security policies, procedures or guidelines relevant to each of the RCHT sites they may operate from.

6. Standards and Practice

6.1. Risk Management

- 6.1.1. All areas, as appropriate, that contain any items, information or persons that may be deemed as sensitive should be protected by either physical or technological security measures. Managers of such areas are responsible for ensuring that suitable preventative measures are taken which will minimise the exposure to any form of security risk.
- 6.1.2. Where a risk/hazard has been identified by a ward or department Manager it will be their responsibility to carry out a risk assessment.
- 6.1.3. Managers, who require advice about risk assessment for their area of responsibility, or advice on the changes of use of an area, should contact the Trust Security Lead (LSMS).
- 6.1.4. Risks should be managed in accordance with the Trust's Risk Assessment and Management Strategy and Policy. The development of Action Plans associated with these risks will be carried out by the ward or department Manager.
- 6.1.5. Where risk assessments indicate a risk of a security incident occurring, managers should employ the appropriate security measures in order to reduce the risk. This may include the review of reviewing access measures to the area systems, security procedures for staff, the design of reception areas, fitting panic buttons in high risk areas; or the issue of personal attack alarms. These should be included in risk assessment and action plans.
- 6.1.6. The Trust Security Lead (LSMS) should be informed and consulted of any related action plans which identify improvements that are required to improve security.

6.2. Fraud

- 6.2.1. Fraud is not within the remit of the Trust Security Lead (LSMS), the Trust has Local Counter Fraud Specialists (LCFS) for this purpose.
- 6.2.2. However, fraud is a serious offence and diverts Trust funds away from patient care. Allegations of fraud are taken seriously by the Trust and offenders face both disciplinary action and prosecution.

- 6.2.3. The Trust's Standing Financial Instructions must be followed at all times.
- 6.2.4. Staff suspecting fraud should contact the Trust Counter Fraud Specialist on 01872 258057.

6.3. Reporting Of Crime and Security Incidents

- 6.3.1. All staff have a responsibility to report security incidents or near misses, via the Datix system, in accordance with the Trust Procedure for the Reporting of Criminal and Security Incidents (see [Appendix 5](#)).
- 6.3.2. Staff should be aware that early and accurate reporting of crime and security related incidents provide the Trust with a means of combating further similar incidents.
- 6.3.3. The Security Services website provides direct links to police reporting services as a partner service. These links are intended to support staff in fulfilling their duty to report criminal activity promptly and appropriately and the link is not available to the general public.

6.4. Working in Partnership with the Police

- 6.4.1. The Trust has a working partnership with the Devon and Cornwall Police. Police Community Support Officers (PCSO's) and the Local Beat Manager regularly patrol the Trust hospitals. There is a police single point of contact (SPOC) nominated for the Royal Cornwall Hospital and West Cornwall Hospital.
- 6.4.2. The Trust Security Lead (LSMS) will maintain regular liaison between the PCSO's, and Police Officers on specific matters involving the Trust.
- 6.4.3. The Police will be given adequate facilities and proper assistance for the conduct of any investigation on Trust property.

6.5. Sanctions

- 6.5.1. Any violence or abuse directed at NHS staff by patients, relatives or members of the public is unacceptable. This Trust, in line with the NHS, is firmly of the view that all those who work in, or provide services for the NHS, have the right to do so without the fear of violence or abuse.
- 6.5.2. There is a range of sanctions that can be applied to those who commit criminal damage, theft, assault or other crimes against the NHS and NHS staff, whether they are patients, members of the public or staff.
- 6.5.3. In terms of patients and the public, this primarily consists of the criminal and civil law. When antisocial behaviour takes place in a healthcare setting, administrative action can also be considered; for example, the issue of an Acknowledgement of Responsibilities Arrangement (ARA), or the withdrawal of treatment.
- 6.5.4. For staff and professionals, disciplinary and professional regulatory processes may be appropriate in addition to criminal and civil sanctions.

- 6.5.5. Information about persons who have displayed unacceptable behaviour towards Trust staff will be shared with other NHS bodies and Government agencies that we currently provide services with, for the purposes of their protection and health and safety. This information is also recorded on the Patient Administration System for 12 months to alert staff of an individual's unacceptable behaviour. Notifications to the relevant staff and partner organisations will be coordinated by the Trust Security Lead (LSMS), ensuring timely and appropriate dissemination of information.

6.6. Protection of Critical Assets

Trust critical assets must be adequately secure. Managers must be aware of any national or local increase in the threat which may possibly have an effect on their area of responsibility. A contingency procedure should be formulated to provide for business continuity (disaster recovery) in the event of an incident occurring to critical assets within the Trust. The business continuity work is led by the Head of Emergency Preparedness and Resilience (EPRR).

6.7. Site Security

- 6.7.1. Royal Cornwall Hospital – For the day-to-day security of the Royal Cornwall Hospital we have a 24/7 Security Officer Team and Night Security at our designated main entrances.
- 6.7.2. West Cornwall Hospital and St. Michaels Hospital - The day-to-day security at West Cornwall Hospital site and St Michael's Hospital sites remains the responsibility of the relevant Hospital Manager, who will report to Trust Security Lead (LSMS) and/or the Security Management Director (SMD) on all matters relating to security.

6.8. Building Security

Building security throughout the Trust remains the responsibility of the individuals who work in each room/area of each building. This should be achieved through the co-operation of every individual, under the direction of the building manager or supervisor who is responsible for the room/area concerned.

6.9. Personal Security of Staff

The Trust has introduced measures to protect the personal security of its employees which include:

- The installation of security and panic attack alarms in departments where a need has been identified.
- A dedicated telephone monitoring service for the protection of community lone workers.
- Access control measures.
- Use and promotion of CCTV systems.
- The use of appropriate sanctions to support staff.

6.10. **Asset Management**

In compliance with the NHS financial management regulations an asset register of all items valued at over £5,000 is maintained by the Finance Department.

6.11. **Security Marking of Valuable Equipment**

Valuable and/or attractive items of equipment should be security marked to deter theft and assist with identification in the event of the item being recovered.

6.12. **Recovery of Losses**

- 6.12.1. The Trust is committed to the recovery of loss by holding to account those who cause loss to the Trust through criminal damage or theft.
- 6.12.2. The Trust will work closely with the Police, the Crown Prosecution Service or other agency such as Her Majesty's Revenue and Customs (HMRC) in order to achieve this.

6.13. **Identification of Personnel**

6.13.1. **Identification Cards**

- 6.13.2. All staff employed by the Trust will wear their identification card at all times whilst on duty. It is the responsibility of every member of staff to ensure that their identification card is valid and displays a current image of themselves. It is a requirement that the identification card is displayed on the person in a manner that it can be seen and read by the average person.
- 6.13.3. Staff members are positively encouraged to politely challenge anyone who does not wear identification when in non-public areas of Trust property. Managers should give active support to any member of staff experiencing difficulty through carrying out the challenging procedure.
- 6.13.4. If a temporary form of identification is required this must be issued by the Security Services ID Badge Service 2. Locally produced departmental identification cards are not permitted under any circumstances.
- 6.13.5. [Appendix 4](#): Security Identity Badge Protocol provides further guidance on this subject.

6.13.6. **Visitor Access**

Visitor access to Trust hospitals is permitted only through designated authorised entry points. Staff should ensure visitors are directed to these approved access routes when entering Trust premises. This policy is to be enforced for patient, visitor and staff safety. Any visitor wishing to visit a patient outside normal visiting times should be advised to make prior arrangements with the ward/department. Protected mealtimes should be adhered to.

² The Estates Department are authorised for the production of Contractor ID Badges

6.14. Conflict Resolution Training

If frontline NHS staff whose work brings them into contact with members of the public or whose work may expose them to situations that may become volatile and confrontational will receive training in conflict resolution. The training will include non-physical intervention techniques on managing and de-escalating potentially violent incidents within the work environment.

6.15. Security of Computerised Information

The Director of CITS is responsible for formulating procedures and guidelines relating to the security of computerised information within the Trust.

6.16. Security of Health Records

The procedures and policy relating to the handling and storage of health records for all of the Trust hospital sites are contained in the Management of Information, Records and Data Quality Policy. The Records Services Manager is responsible for the correct procedures and storage of health records for all hospitals in the Trust.

6.17. Closed Circuit Television (CCTV)

Closed Circuit Television systems are in operation throughout the Trust. Separate Trust guidance has been produced which identifies the purpose, accountability, management and monitoring responsibilities for the system (CCTV Code of Practice).

6.18. Purchase of Security Systems

6.18.1. All Care Groups/Departments must consult with the Trust Security Lead (LSMS) and the relevant Estates Department Manager before purchasing security equipment or systems (such as automated access control systems, including video/intercom systems and swipe card readers; CCTV, security lighting, and intruder alarms).

6.18.2. Equipment purchased must conform to the Trust specification for compatibility with existing systems and compliant with other statutory regulations and guidance. Initial requests to be raised on the Estates micad system.

6.19. Bomb Threat/Suspect Packages

There is a separate policy, the Trust's Bomb Threat Policy which provides further information of how to manage a bomb threat. A quick checklist and guide for staff "Procedure for Staff Receiving a Telephone Bomb Threat or finding a Suspicious or Unattended Package" can be found at [Appendix 6](#) of this policy.

6.20. Lockdown

- 6.20.1. Lockdown is the process of controlling the movement and access - both entry and exit of people. A lockdown is achieved through a combination of physical security measures and the deployment of security and other personnel.
- 6.20.2. A lockdown may be implemented by the Royal Cornwall Hospitals NHS Trust as part of a security incident or the major incident plan. This may be in partnership with other organisations both NHS and external e.g. due to Police intelligence.
- 6.20.3. The ability of NHS Acute Trusts to lock down their site or buildings fits in with their statutory responsibilities as Category One Responders, as defined by the Civil Contingencies Act 2004.
- 6.20.4. For more information about Lockdown, refer to the Trust Lockdown Policy.

6.21. Escalation of Security Incident

- 6.21.1. In the event of a security threat level being significantly increased, the Trust will escalate the threat in line with the Critical or Major Incident Plan.
- 6.21.2. The Clinical Site Managers and Senior Executive and Management teams (on Call) via the Incident Coordination Centre have the authority to increase the level of security resources and responses by using officers from the in house security response team or by providing manpower from external security resources.
- 6.21.3. The relevant contact details for increasing the numbers of internal and/or external security officers will be available in the security control room.

6.22. Firearm or Weapons Attack

- 6.22.1. National Counter Terrorism policing is providing advice to the public on the steps that they can take to keep themselves safe in the rare event of a firearm or weapons attack.
- 6.22.2. In the rare event of a firearms or weapons attack staff should follow the National Counter Terrorism policing guidance:
 - RUN - Run to a place of safety. It is a far better option than to surrender or negotiate. If there is nowhere to go then,
 - HIDE – It's better hide than to confront. Remember to turn your phone to silent and turn off the vibrate option. Barricade yourself in if you can. Then finally and only when it's safe to do so,
 - TELL - Tell the police by calling 999.
- 6.22.3. For further guidance on how to stay safe from a firearms and weapons

attack including the 'Stay Safe' short film follow this link: [Run-Hide-Tell Advice](#).

6.22.4. For a range of short films providing advice and information of how to 'Stay Safe', follow this link: [How to deal with terrorist incidents](#).

6.23. Managing Security Alerts

The Trust will issue National and Regional NHS England security alerts to relevant staff groups and take action to raise awareness of the security risks and incidents identified in the alerts.

6.24. Training

The Trust Board is committed to delivering a staff training programme that encourages and develops a pro-active security culture. This will contain practical crime prevention advice and techniques and induction training, security awareness displays, conflict resolution and physical intervention training. This training will assist with the provision of a safe and secure environment for all.

7. Dissemination and Implementation

- 7.1. Managers need to ensure that the staff they manage are aware of this policy. This should be achieved by highlighting and discussing the issue at Departmental Induction for newly appointed staff and through regular performance review process for existing staff.
- 7.2. The document will be stored electronically on the document library on the Trust internet/intranet site.
- 7.3. The trust will continue to raise staff awareness annually by publicising the existence of the policy through a variety of methods which may include: Trust communications Team Talk, All user email, payslip message, screen saver, posters/leaflets.

8. Monitoring compliance and effectiveness

Information Category	Detail of process and methodology for monitoring compliance
Element to be monitored	The Local Security Management Specialist will monitor and review all security incidents across the Trust.
Lead	The Trust Security Lead (LSMS) - Local Security Management Specialist.
Tool	The Trust Security Lead (LSMS) work plan that highlights all security management work is monitored as follows: - Internally by the Director of Estates and Facilities, the Security Management Director (SMD), the Non-Executive Director (NED) and the Trust Board. - Externally by the NHS England, Health and Safety Executive

	and the Care Quality Commission.
Frequency	The Trust Security Lead (LSMS) will produce an Annual Report to the Security Management Director (SMD) and the Non-Executive Director (NED). This report is also provided to Trust Executive Board.
Reporting arrangements	Reports are made to the Health and Safety Committee meetings as appropriate. The Non-Executive Director (NED meeting) will monitor the implementation of this policy in terms of effectiveness and performance by reviewing information, incidents and reports and the annual report to the Trust Executive Board.
Acting on recommendations and Lead(s)	The Trust Security Lead (LSMS) will undertake subsequent recommendations and action planning for any deficiencies that are identified, together with a timeframe for completion.
Change in practice and lessons to be shared	Any changes that are identified and which require action will be taken to the Health and Safety Committee and any other group/committee that is relevant. Any lessons learnt will be shared with all relevant stakeholders.

9. Updating and Review

- 9.1. This policy will be reviewed every 3 years or earlier in view of developments which may include legislative changes, national policy instruction (NHS or Department of Health) or Trust Board decision.
- 9.2. Revisions will be made ahead of the review date if there are any changes to legislation or organisational structure which may impact this policy.
- 9.3. Changes or revisions made will be taken through the standard consultation, approval and dissemination processes.

10. Equality and Diversity

- 10.1. This document complies with the Royal Cornwall Hospitals NHS Trust service Equality and Diversity statement which can be found in the [Equality Diversity And Inclusion Policy](#) or the [Equality and Diversity website](#).
- 10.2. Equality Impact Assessment

The Initial Equality Impact Assessment Screening Form is at Appendix 2.

Appendix 1. Governance Information

Information Category	Detailed Information
Document Title:	Security Policy V7.0
This document replaces (exact title of previous version):	Security Policy V6.0
Date Issued/Approved:	September 2025.
Date Valid From:	December 2025.
Date Valid To:	December 2028.
Directorate / Department responsible (author/owner):	Natasha Quick, Trust Security Lead (LSMS).
Contact details:	01872 252147.
Brief summary of contents:	Security Policy, Identity Badge, Reporting Security Incidents, Closed Circuit Television. Purchase of Security Systems, Lockdown, Escalating Security Incidents, Managing Security Alerts, Bomb Threats, Risk Management, Fraud, Reporting Security Incidents, Police Partnership, Sanctions, Protection of Critical Assets, Site Security, Building Security, Personal Security of Staff, Asset Management, Security Marking, Recovery of Losses, Firearm or Weapons Attack, Identification of Personnel, Visitor Access, Conflict Resolution, Security of Computerised Information, Security of Health Records, CCTV, Purchase of Security Equipment.
Suggested Keywords:	Security Policy, Identity Badge, Access Control, Reporting, Security Incidents.
Target Audience:	RCHT: Yes CFT: No CIOB ICB: No
Executive Director responsible for Policy:	Brian Johnson, Director of Estates and Facilities.
Approval route for consultation and ratification:	Health and Safety Committee.

Information Category	Detailed Information
General Manager confirming approval processes:	Natasha Quick, Trust Security Lead (LSMS).
Name of Governance Lead confirming approval by specialty and care group management meetings:	Debbie Price, Business and Security Systems Manager.
Links to key external standards:	The NHS Security Management Manual.
Related Documents:	Guide to good practice for the Security of Premises (Appendix 3 of this policy). Security Identity Badge Protocol. Procedure for the Reporting of all Criminal and Security Incidents. Procedure for staff Receiving a Telephone Bomb Threat or Finding a Suspicious or Unattended Package. Management of Violence and Aggression Policy. Lone Working Policy. Lockdown Policy. Bomb Threat Policy. Restrictive Practice Policy.
Training Need Identified?	Yes, The Learning and Development department have been informed.
Publication Location (refer to Policy on Policies – Approvals and Ratification):	Internet and Intranet.
Document Library Folder/Sub Folder:	Estates and Facilities / Security.

Version Control Table

Date	Version Number	Summary of Changes	Changes Made by
February 2008.	V1	Policy rewritten.	Barry Sobey Security Advisor.
June 2008.	V1.1	Minor updating required on coversheet and in body of policy. Clinical Governance and Trust Librarian consulted.	Stuart Harrison LSMS.

May 2009.	V2	Updating of policy to include details of CFSMS, role of SMD and LSMS, referral to Lockdown procedure and Risk management. Clinical Governance. Director Estates and Facilities and Librarian consulted.	Stuart Harrison LSMS.
June 2010.	V3	Updating of policy on coversheet, NHLA monitoring and compliance, add lock down.	Stuart Harrison LSMS.
May 2011.	V3.1	Reformatted to comply with Policy on Policies.	Andrew Rogers Corporate Records Manager.
May 2013.	V4.0	Policy rewritten.	Paul Dixon- Security Manager LSMS.
June 2016.	V4.1	Policy Updated.	Paul Dixon- Security Manager LSMS.
June 2019.	V5.0	Policy Updated, Firearm or Weapons Attack paragraph added.	Paul Dixon- Security Manager LSMS.
August 2022.	V6.0	Policy Updated and minor amendments made.	Paul Dixon - Head of Security / LSMS.
August 2025.	V7.0	Policy Updated and minor amendments made.	Natasha Quick, Trust Security Lead (LSMS).

All or part of this document can be released under the Freedom of Information Act 2000.

All Policies, Strategies and Operating Procedures, including Business Plans, are to be kept for the lifetime of the organisation plus 6 years.

This document is only valid on the day of printing.

Controlled Document.

This document has been created following the Royal Cornwall Hospitals NHS Trust [The Policy on Policies \(Development and Management of Knowledge Procedural and Web Documents Policy\)](#). It should not be altered in any way without the express permission of the author or their Line Manager.

Appendix 2. Equality Impact Assessment

Section 1: Equality Impact Assessment (EIA) Form

The EIA process allows the Trust to identify where a policy or service may have a negative impact on an individual or particular group of people.

For guidance please refer to the Equality Impact Assessment Policy (available from the document library) or contact the Equality, Diversity, and Inclusion Team
richt.inclusion@nhs.net

Information Category	Detailed Information
Name of the strategy / policy / proposal / service function to be assessed:	Security Policy V7.0.
Department and Service Area:	Estates and Facilities / Security.
Is this a new or existing document?	Existing.
Name of individual completing EIA (Should be completed by an individual with a good understanding of the Service/Policy):	Trust Security Lead (LSMS).
Contact details:	01872 25 2417.

Information Category	Detailed Information
1. Policy Aim - Who is the Policy aimed at? (The Policy is the Strategy, Policy, Proposal or Service Change to be assessed)	A robust security policy for the Trust.
2. Policy Objectives	To promote a pro security culture throughout the Trust.
3. Policy Intended Outcomes	Clear concise guidelines to be followed by all staff.
4. How will you measure each outcome?	Through training, the Trust risk reporting system (Datix), Police crime statistics.
5. Who is intended to benefit from the policy?	All staff, visitors, patients, contractors and volunteers (everyone).

Information Category	Detailed Information
6a. Who did you consult with? (Please select Yes or No for each category)	- Workforce: Yes - Patients/ visitors: No - Local groups/ system partners: No - External organisations: No - Other: No
6b. Please list the individuals/groups who have been consulted about this policy.	Please record specific names of individuals/ groups: Health and Safety Committee.
6c. What was the outcome of the consultation?	Approved.
6d. Have you used any of the following to assist your assessment?	National or local statistics, audits, activity reports, process maps, complaints, staff, or patient surveys: No.

7. The Impact

Following consultation with key groups, has a negative impact been identified for any protected characteristic? Please note that a rationale is required for each one.

Where a negative impact is identified without rationale, the key groups will need to be consulted again.

Protected Characteristic	(Yes or No)	Rationale
Age	No	This Policy does not impact on age.
Sex (male or female)	No	This Policy does not impact on gender.
Gender reassignment (Transgender, non-binary, gender fluid etc.)	No	This Policy does not impact on gender reassignment.
Race	No	This Policy does not impact on race.
Disability (e.g. physical or cognitive impairment, mental health, long term conditions etc.)	No	This Policy does not impact on disability.
Religion or belief	No	This Policy does not impact on religion or beliefs.
Marriage and civil partnership	No	This Policy does not impact on marriage and civil partnership.

Protected Characteristic	(Yes or No)	Rationale
Pregnancy and maternity	No	This Policy does not impact on pregnancy and maternity.
Sexual orientation (e.g. gay, straight, bisexual, lesbian etc.)	No	This Policy does not impact on sexual orientation.

A robust rationale must be in place for all protected characteristics. If a negative impact has been identified, please complete section 2. If no negative impact has been identified and if this is not a major service change, you can end the assessment here.

I am confident that section 2 of this EIA does not need completing as there are no highlighted risks of negative impact occurring because of this policy.

Name of person confirming result of initial impact assessment: Debbie Price, Business and Security Systems Manager.

If a negative impact has been identified above OR this is a major service change, you will need to complete section 2 of the EIA form available here:

[Section 2. Full Equality Analysis](#)

Appendix 3. Guide to Good Practice for the Security of Premises

1. Introduction

To enable the Trust to be successful in its security aims it is important that staff share in the commitment to maintain a secure environment. This can be carried out by following good practice and thereby reducing the risk.

2. Responsibilities

All staff are responsible for ensuring that they take adequate precautions to protect their own personal property, together with that of patients and the Trust. Staff should ensure that they always report crime or security breaches as soon as possible.

3. Preventative Measures

3.1. Staff can be very effective in deterring aspects of crime, if they apply the following basic, but effective, principles during their working day/night:-

3.1.1. If you see suspicious individuals or groups in non-public areas or causing concern, challenge them politely by asking them if they require any help and noting their response. If they appear nervous, unsure, or over confident and you are not happy with their response, inform your line manager and/or the on duty security officers on 2999 immediately.

3.1.2. When making a challenge never place yourself at risk, and always be polite. If you challenge someone who states they are a member of staff, ask to see their identification and remind them that Trust identification badges should be worn at all times. A simple "Can I help you" can prevent would be offenders from committing crimes in that area.

3.1.3. Always lock offices, rooms or store areas that are not in use. This measure will deter the opportunist thief.

3.1.4. Never leave personal items such as handbags, wallets or clothing etc. in view from windows or open doors. Always lock attractive items away.

3.2. Theft is not always the motivation, and, unfortunately, attacks on staff and arson are not unheard of in healthcare establishments. Following the above guidance may help to deter any person with a violent intent towards either staff or patients.

4. Room Security

Any room that contains valuable or vulnerable items of equipment should remain locked at all times when not being used. The following good practice will assist in deterring or denying a potential criminal valuable information or access:-

4.1. Always draw curtains or lower blinds as you leave your office in the evening.

4.2. Lock all sensitive documentation or data media away and out of sight.

4.3. When establishing an office environment, wherever possible plan for any

attractive, moveable items to be situated in a position that is out of view of the opportunist thief.

- 4.4. Always double check that the windows are firmly closed and that the window catch has been placed into the locked position (especially for sash type windows). Any broken catches or locks should be reported to the Estates Department immediately.
- 4.5. At the end of the working day, the last person to leave, or the person responsible, should ensure that the relevant alarms are set and double check that all doors and windows within their area of responsibility have been locked.

5. Ward Security

- 5.1. Wards have the added burden of providing security for equipment, staff and patients, including infants. Patients can, and do, arrive at the hospital carrying large amounts of money, or wearing expensive jewellery, which has to be removed as part of a medical requirement.
- 5.2. Particular attention should be made by ward staff to maintain security in the areas already mentioned in this policy, but the following additional guidelines should also be followed:-
 - 5.2.1. Always ensure that the correct procedure is used when dealing with patient's belongings and valuables. The Patient Property Procedure has full details regarding this area.
 - 5.2.2. Always ask anyone who looks unsure as to where they are, or as to who they are visiting, to identify their intentions.
 - 5.2.3. If you have any doubts about the identity or intentions of any visitor, contact your Line Manager or the on-duty Security Officers on 2999.

6. Staff Residential Campus

- 6.1. Staff who live on site in the residences have a responsibility to their neighbours living in the same accommodation and should ensure that their actions do not put others at risk.
- 6.2. Staff accommodated in the residences should follow all the above guidance and should contact the on-duty Security Officers on ext. 2999 for emergencies or ext. 2468 for non-emergencies, if they are aware of any of the following:-
 - 6.2.1. Any person who is displaying suspicious behaviour, lurking, or appears to be lurking around the residences, i.e. peering into rooms or trying doors.
 - 6.2.2. Any person who is acting suspiciously in the vicinity of the residency cars or car parks. Please also notify the car parking contractors.

Appendix 4. Security Identity Badge Protocol

1. Introduction

Security is an integral part of patient care and an identification badge system is a key element in providing a comprehensive security administration. It is vital to be able to identify and recognise fellow staff and individuals with a genuine reason for being on the premises. This can be achieved by ensuring that all applicable staff wear their identity badges at all times whilst on the Trust premises. Also by empowering and encouraging staff and patients to challenge anyone not wearing a badge.

2. Protocol Statement

On commencement of employment, all members of staff will be issued with a Trust identification badge. Any employees of external agencies requiring access to Trust's premises, in the course of their official duties, will adhere to the Trust Identification Badge Protocol. When on duty or working on the Trust premises, the identification badge must be worn at all times and be clearly visible.

3. Scope

- 3.1. There are ID badge designs relevant to the following categories of staff and this Protocol will apply to:
 - 3.1.1. All directly employed and attached staff, temporary or permanent.
 - 3.1.2. Kernowflex staff.
 - 3.1.3. Agency staff.
 - 3.1.4. Official Visitors.
 - 3.1.5. Contractors.
 - 3.1.6. Voluntary organisations.
 - 3.1.7. External agencies including students.
- 3.2. The background colour of the photograph on all staff badges will be the corporate colour of blue. Where photographs have any other colour background for their photograph, the individual member of staff will ensure their badge is replaced as soon as possible.

4. Responsibilities

4.1. Management Responsibilities.

- 4.1.1. Managers are responsible for ensuring that all their staff are aware of the Trust's Identification Badge Protocol and that badges are worn and clearly visible at all times.
- 4.1.2. The line manager is responsible for ensuring that the identification

badge is returned to the Security ID Badge Service upon termination of a member of staff's employment or, in the case of an official visit, at the end of that visit.

- 4.1.3. All managers are expected to encourage and support staff to challenge anyone not wearing an identification badge.
- 4.1.4. Managers must ensure that any lost or damaged badges are reported to the Security ID Badge Service (rch-tr.IDBadge@nhs.net) and arrangements are made for a replacement badge to be issued.
- 4.1.5. Managers must ensure that arrangements are in place for providing identification badges for official visitors or contractors working in their areas of responsibility.
- 4.1.6. Managers are responsible for monitoring the implementation and adherence to the Security Identity Badge Protocol in their areas of responsibility.

4.2. Staff Responsibilities.

- 4.2.1. It is the responsibility of individual staff to ensure that the identification badge is worn at all times whilst on duty and that it is clearly visible.
- 4.2.2. It is the responsibility of individual staff to ensure that the badge is kept in date, and secure when not being worn.
- 4.2.3. Lost or damaged badges must be reported to the member of staff's line manager and rcht.accesscontrol@nhs.net immediately, then a replacement should be obtained from the Security ID Badge Service.
- 4.2.4. All staff must ensure that the image on their ID badge is clear and fit for the purpose of identification. If the photo is damaged or worn the badge must be renewed immediately.
- 4.2.5. The identification badge must be worn in the holder provided, with either a Trust lanyard or clasp used to display it on the individual.
- 4.2.6. Staff are encouraged, and will be supported, to challenge and question people not wearing identification, particularly if seen in non-public areas, or are causing concerns.
- 4.2.7. It is recognised that it may not be appropriate for some clinical staff working in controlled areas, i.e. Theatres, to wear the identification badge. At these times, the badge should be on the person and visibly displayed once the controlled area is left.

4.3. Security ID Badge Service Responsibilities

- 4.3.1. The Security ID Badge Service is responsible for the issuing of identification badges to all new members of staff on the first day of appointment.
- 4.3.2. A central database will be maintained within the Security ID Badge

Service that will register all names, photographs and details of legitimate staff, official visitors and voluntary staff.

4.3.3. The Security ID Badge will be replaced:

- Every seven years for permanent staff.
- If the badge is damaged or mislaid.
- If there is significant change to the employee's status.
- If the photograph is not taken with the blue corporate background.

4.4. Trust Security Lead (LSMS) Responsibilities

The Trust Security Lead (LSMS) will be responsible for ensuring that monitoring and auditing takes place to ensure compliance with the Security Identity Badge Protocol. The Trust Security Lead (LSMS) will carry out regular security checks on the identification badge database.

4.5. Access Control Service

- 4.5.1. The Trust Identity Badge is integral to the Access Control system deployed throughout the Trust.
- 4.5.2. Each time a card is used in a door reader it presents an audit trail of its use. This trail gives the time and door location that the card was used.
- 4.5.3. Staff are not to allow other members of staff to use their cards at any time as this will present an incorrect audit trail which could be misleading in any disciplinary or criminal enquiry.
- 4.5.4. All staff identity badges will have an expiry date displayed on them. This date will automatically disable the access levels allocated to the badge.
- 4.5.5. A list of all staff leaving the Trust will be provided by Cornwall IT Services on a weekly basis. The badges of all leavers on the list will be disabled.
- 4.5.6. Persons issued with an Identity Badge who are visiting the Trust for short periods or working on short term contracts will have the actual date of expiry that their visit/contract ends displayed upon their Identity Badge.

5. Contractors

All 'Contracts of Engagement' will contain a clause, which stipulates that the Contractor must, when on site, adhere to the Security Identity Badge Protocol.

Breach of this policy will result in the removal of the offending contractor's employee from the site. Specific contractor's identification badges will be issued via

departmental procedures agreed with the Trust Security Lead (LSMS) and the Security ID Badge and Access Control Services.

6. Official Visitors

Official visitors must be made aware that the Security Identity Badge Protocol must be adhered to. Official visitors will be issued with a specific visitor identification badge, via departmental procedures agreed with the Trust Security Lead (LSMS) and the Security ID Badge and Access Control Services. Each individual visitor must present proof of identity before a badge can be issued.

7. Voluntary Organisations

Voluntary organisations, that work closely and on a regular basis with the Trust, will be requested to issue their volunteers with specific Volunteer identification badges. These personnel will be expected to comply with the Security Identity Badge Protocol when on Trust's premises.

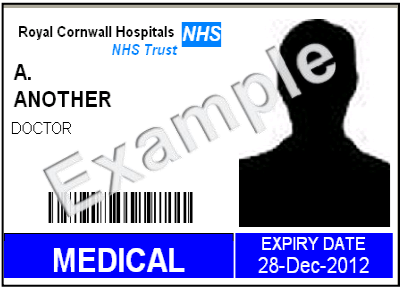
8. External Agencies

Staff belonging to external agencies, which are required to work on Trust premises, will be required to wear their own organisation's identification badge. This badge must be worn at all times when on Trust premises and be clearly visible.

9. Enforcement

Patients and visitors must recognise that when they enter the Trust's hospitals, they are entering premises that place a high priority on security. They must have confidence that the system will keep them secure and that staff are there to help. The Trust will publish and signpost the fact that a security identification system is in use and that visitors can expect to be challenged. Breach of the Security Identity Badge Protocol by staff could result in disciplinary action.

ID Badge Designs 2025 - Example Badges



RCHT Staff Barcode

RCHT Attached Staff



Kernowflex Staff

Contractor with Photo



RCHT Temporary Visitor

RCHT Volunteer

Appendix 5. Procedure for Reporting Criminal and Security Incidents

1. Introduction

Providing a safe and secure environment for patients, staff and visitors is an essential feature in the delivery of a high quality health care service. To enable the Trust to meet these requirements it is important that all incidents relating to crime and security are reported promptly. This will enable the Trust to be supportive to staff and to fulfil the commitment to manage security at an appropriate level. It will provide the means for the Trust to identify areas of concern and to take action to reduce any further risk to such areas. Reporting of any criminal or security incidents will also allow the Trust to evaluate exactly how much, in financial terms, is lost through theft and vandalism.

2. Responsibility

All employees of the Trust are responsible for the reporting of crime or breaches of security.

3. What Should Be Reported

All incidents of theft, violence, and breaches of security should be reported via the Datix system and/or direct to the Police.

4. Method Of Reporting

- 4.1. If staff see or are aware of a crime, or a breach of security being committed, they have a responsibility to report this.
- 4.2. Initially the report should be made as follows:
 - By dialling 2999 for an immediate response from the 24/7 Security Response team (RCH only).
 - By notifying their immediate manager or senior person on duty.
 - By notifying the Trust Security Lead (LSMS).
 - By direct notification to the Police in an emergency.
 - By using the online Devon and Cornwall Police form, a link to which can be found on the [Useful policies and links | Intranet - Royal Cornwall Hospitals Trust](#). page of the security services website.
- 4.3. The initial verbal or email report must always be followed up with a Datix as soon as possible and will be investigated by the appropriate department.
- 4.4. Incidents which involve violence and aggression should be reported on Datix as soon as possible and will be investigated by the appropriate department.
- 4.5. All security related Datix reports will be reviewed by Security Services, with support and guidance given to departments to ensure appropriate action is taken.

5. Police Involvement

If an incident is serious enough to require the presence of the Police, do not hesitate to contact them immediately, especially where violence is threatened. In most cases the Trust Security Lead (LSMS) will involve the Police.

6. Summary

- 6.1. The system of reporting incidents allows you to help the Trust to assess the threat and to identify crime trends. It also provides an assessment of the financial costs to this Trust incurred by criminal activity. By reporting incidents immediately, you are allowing the Trust to plan for your safety.
- 6.2. If at any time you want to speak in strict confidence, you can talk to the Trust Security Lead (LSMS) or other senior manager as appropriate who will be willing to meet with you (including night shift staff).

Appendix 6. Procedure for Staff Receiving a Telephone Bomb Threat or finding a Suspicious or Unattended Package

1. Introduction

- This procedure has been produced to give members of staff sufficient guidance to follow if they should receive a telephoned bomb threat or find a suspicious package. It has been produced to respond to several incidents that have occurred in recent years, when NHS establishments have been the targets of advised forthcoming terrorist attacks.
- Bombs are designed to cause death, injury or damage. They can be made to look like almost anything, alternatively they can be so small that they can be concealed in almost anything. Bombs have been hidden in lorries, vans, cars, briefcases, handbags, holdalls and even in shoes. They have been hidden in litter bins and even in display shelves in shops, all of these areas appear in a hospital environment.
- Good housekeeping both inside and outside the hospital will reduce the opportunity for an explosive device to be planted. Staff should remain vigilant and be prepared to report anything they feel is suspicious. It is safer to report than not to, even if the outcome of any follow up action is that nothing is found.
- Within the hospital it is important to reduce the number of places in which articles can be hidden. All rooms, stairways, corridors, and public areas should be kept clear and tidy. Unoccupied rooms and store cupboards should be kept locked.
- Outside areas of the hospital, especially where deliveries are made, should also be kept clear and tidy. Every effort should be made to reduce the opportunity for articles to be deposited which could conceal an explosive device.
- NHS premises themselves can be vulnerable to bomb attacks threats and hoaxes. This procedure incorporates the best and most up-to-date advice from experts in Government and the Police Service, as contained in the 1994 Home Office publication 'Bombs – Protecting People and Property'. This 1994 documentation is expected to be superseded, (during the life of this policy document), by the requirements of emerging legislation and up-to date advice, as a result of The Terrorism (Protection of Premises) Act 2025 (Martyn's Law).
- A threat may be written or, more likely, be received as a telephone call. Developments and improvements in telephone systems e.g. direct dialling inwards (DDI) means that it will not necessarily be the switchboard staff that will receive the threat. A member of staff in an office, on a ward, or even in the residences may receive the threat.

How a person receiving a threat responds can be the key to the preservation of life and property: "The help and support we (The Police) get from the public is a vital part of working together to combat terrorism. We urge everyone to remain vigilant, and if you do see anything suspicious then please report it, in confidence, to police via [gov.uk/ACT](https://www.gov.uk/ACT). It won't ruin lives, but it may well save them.

Always call 999 in an emergency".

2. Guidance for Staff Receiving Bomb Threats

- If you receive a telephone threat, it is important to remain calm and to record as much detail about the call and associated background noises as possible.
- If the threat is from a large terrorist organisation, they will authenticate the threat by a coded password that will be recognised by the police. To assist you with recording the threat, please use the telephone checklist in the bomb policy. If it is not possible to use the checklist at the time of the call, take notes on rough paper and fill in the checklist later. It will help to prompt your memory for helpful details.
- Once you have taken and recorded the message, inform the following immediately:

INFORM THE POLICE BY DIALLING (9)999	Extension
Royal Cornwall Hospital.	
During office hours:	
Local Security Management Specialist.	Ext 2147
Senior Manager on-Call.	Ext 4444 via Switchboard
Facilities Helpdesk (Ask for Security Services).	Ext 2468
Clinical Site Manager.	Ext 4444 via Switchboard
Outside office hours:	
Clinical Site Manager.	Ext 4444 via Switchboard
Senior Manager on Call.	Ext 4444 via Switchboard
West Cornwall Hospital:	
During office hours:	
Nurse Manager.	Ext 4100
Outside office hours:	
Senior Night Nurse.	Ext 4444 via Switchboard
St Michael's Hospital:	
At all times:	
Contact 0 0 bleep holder.	Page 0 0

3. Guidance for Staff Finding a Suspicious Object or an Unattended Package

A suspicious object is an item, which might contain a bomb. It may look out of place or may be able to be accounted for. Any suspicious package or box found must be treated with extreme caution, and the police notified immediately, followed by the appropriate manager as detailed in the Bomb Threat Policy.

4. Management Action to be Taken on the Notification of a Bomb Threat or on the Report of a Suspicious Object or an Unattended Package

- If, as a manager, you receive notification of a bomb threat or a suspicious object/unattended package, confirm that the police have been informed and that any code words that have been used are passed to them.
- If the code word has been recognised by the police, they will react and you may have to initiate an evacuation of the identified threat area together with the adjoining area and the floor above and below.
- An incident control centre should be designated away from the threat area for briefing staff and the emergency services. Building plans should be made available where possible. The police will give further advice upon arrival.
- If no code was used and there has been an area specified, arrange for a quick search of that area to be carried out, using staff from that area and the security staff. Do not allow anything suspicious to be touched or moved.
- If nothing is found in the specified area, re-brief and broaden the search around the area to be sure that there has not been a mistake by the caller. If there is still nothing found, await the arrival of the police and take their advice when they do arrive.
- If a suspicious object or package is reported or found when searching, immediately initiate an evacuation of the area. Report the findings to the police and await their arrival and then take their advice.
- If nothing is found in the initial quick search, a more thorough search should then be carried out, this time in a more methodical way, paying a lot more attention to detail and probing into smaller areas such as cupboards etc.
- Once you are happy that there is no threat remaining and the police are also certain, the threat should be disregarded and staff advised accordingly.

For further information please refer to the Trust [Bomb Threat policy](#).