

Access Control Policy

V3.0

December 2024

Summary

Access Control

The control of access in a hospital environment is a key element in providing a comprehensive security culture throughout the organisation. The Royal Cornwall Hospitals NHS Trust has installed an electronic access control system which allows movement to be controlled by a card reader system.

Role of Managers in Areas Controlled by an Electronic Control System.

Managers are responsible for ensuring that their area of responsibility is risk assessed and that they fully understand the access and egress requirements of their area.

Managers are responsible for authorising staff to access their area through the electronic control system. They are to assume the role of Departmental Named Authoriser or appoint a member/s of staff to carry out this duty as well as, or on their behalf.

Managers are expected to encourage and support staff to challenge anyone who they do not recognise who attempt to follow them into a restricted access area.

Table of Contents

Summary	2
1. Introduction.....	5
2. Purpose of this Policy/Procedure	5
3. Scope.....	5
4. Definitions/Glossary	6
5. Ownership and Responsibilities	6
5.2. The Local Security Management Specialist (LSMS).....	6
5.3. Role of Managers in Areas Controlled by an Electronic Control System	7
5.4. Departmental Named Authoriser	7
5.5. Role of Staff, Official Visitors, Volunteers, External Agencies (Staff).....	7
5.6. Role of Estates Helpdesk	8
5.7. Access Control and ID Badge Service Responsibilities	8
6. Standards and Practice	9
6.1. Door Control	9
6.2. Identity Badge	10
6.3. Purchase of Electric Access Control System	12
7. Dissemination and Implementation	13
8. Monitoring compliance and effectiveness	13
9. Updating and Review	14
10. Equality and Diversity	15
Appendix 1. Governance Information	16
Appendix 2. Equality Impact Assessment	19

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 control of access in a hospital environment is a key element in providing a comprehensive security culture throughout the organisation. The Royal Cornwall Hospitals NHS Trust has installed an electronic access control system which allows movement to be controlled by a card reader system. Entry into controlled areas is achieved by swiping an authorised Identity Badge through a cardreader. Access levels are allocated to an individual's ID Badge, which is controlled from a central data base administered by the Access Control and ID badge Services.
- 1.2. Each Identity Badge is automatically allocated a minimum level of access to allow staff to move through areas of a hospital where it would be inappropriate for the public to access. ID Badge holders are granted higher access levels to more secure areas in accordance with their work-based activities, access levels are authorised by nominated staff.
- 1.3. The installation of the electronic control system is considered on a risk level basis. The system is installed to strengthen security and protect against risk to staff/ employees, agency employees, patients, visitors and Trust assets.
- 1.4. This version supersedes any previous versions of this document.

2. Purpose of this Policy/Procedure

- 2.1. The purpose of the Access Control Policy is to ensure the following:
- 2.2. To restrict members of the public from gaining access to areas and departments of the hospital without obtaining permission.
- 2.3. To provide a variety of security access or egress levels to control the movement of staff, patients and visitors to and from higher-than-normal risk areas of our hospitals and buildings.
- 2.4. To develop a security awareness culture to encourage staff and patients to challenge anyone not wearing an ID badge in Trust hospitals and premises.

3. Scope

- 3.1. This policy applies to all staff, voluntary organisations, contractors, official visitors and external agencies. It is relevant to all three Trust hospital sites including some standalone premises / sites that have access control measures installed.
- 3.2. Standards, procedures and guidelines, designed to minimise the effects of potential threats are detailed in section 6 of this policy.

- 3.3. Standards, procedures and guidelines will be reviewed and re-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

ID Badge – An identity card issues by the Trust ID Badge Service which displays a clear image of the owner, their name, job title department and care group.

LSMS – Local Security Management Specialist.

Staff – For the purposes of this Policy “Staff” will describe all Trust staff, Kernow Flex and Volunteers.

Official Visitors – Expected visitor/s to the Trust organised by prior arrangement.

Contractors – External company employee working under a written contract on RCHT sites.

External Agencies – Other services or groups required to work or provide a service on Trust premises. i.e. Southwestern Ambulance Service (SWAST) or Plymouth University Students etc.

5. Ownership and Responsibilities

- 5.1. Overall responsibility for security within the Royal Cornwall Hospitals NHS Trust rests with the Chief Executive.

5.2. The Local Security Management Specialist (LSMS)

- 5.2.1. The LSMS will be responsible for monitoring and auditing compliance with the Trust's Access Control Policy. The LSMS will ensure that regular audits of identification badges and the accesscontrol database are undertaken.
- 5.2.2. The LSMS will be responsible for ensuring liaison with the Estates and Strategic teams, to ensure that all access control installations meet the Trust written specification for access control equipment and networks.
- 5.2.3. The LSMS, as subject matter expert, will offer advice to the Trust on the best practice for securing areas where Access Control is required and to support the risk assessment process.

5.3. Role of Managers in Areas Controlled by an Electronic Control System

Line Managers are Responsible for:

- Managers are responsible for authorising staff to access their area through the electronic control system. They are to assume the role of Departmental Named Authoriser or appoint a member/s of staff to carry out this duty as well as, or on their behalf.
- Managers are expected to encourage and support staff to challenge anyone who they do not recognise who attempt to follow them into a restricted access area.
- Managers must ensure that any lost or damaged badges are reported to the ID Badge Service (rch-tr.IDBadge.nhs.net) and arrangements are made for a replacement badge to be issued. (See Para 6.2.5 Lost Identity Badge).
- Managers must ensure that arrangements are in place for providing identification badges for official visitors or contractors working in an area controlled by an electronic control system.

5.4. Departmental Named Authoriser

- A Departmental Named Authoriser should be nominated for each area where an electronic access control system has been installed. This role is usually fulfilled by the manager and another senior member/administrator of the department. The Departmental Named Authoriser will liaise with the Access Control and ID badge Services staff to confirm access requirements of staff to be allowed access to their area. They are to provide e-mail requests for access levels for audit purposes.

The named authorisers will be the point of contact for members of the Access Control and ID badge Services to contact in the event of a query arising from any access requests.

- The Department Named Authoriser will be responsible for removing the access level from any staff, official visitor or contractor no longer requiring access to their area of responsibility.

5.5. Role of Staff, Official Visitors, Volunteers, External Agencies (Staff)

- It is RCHT policy for all staff to be issued with a photo Identity Badge. The ID badge will automatically be authorised to access low risk areas of the Trust where it is inappropriate for the public to have access.

- For some employees it will be a necessary requirement of their work to have access to higher controlled areas. Employees should arrange this access by contacting the relevant departmental named authoriser who will authorise the request if it is deemed applicable.
- Lost badges must be reported to the member of employees' line manager and the ID badge Service immediately. The badge will then be disabled from the access data base and will no longer work with the electronic access control system (see Para 6.2.5 Lost Identity Badge).
- Staff are encouraged, and will be supported, to challenge and question people not wearing identification, particularly if they are in access-controlled department areas.
- The control of contractors' access is covered in the [Management of Contractors Policy](#)

5.6. Role of Estates Helpdesk

- The Estates Helpdesk is responsible for issuing ID Badges to Contractors only where the relevant form has been provided by the Project Manager, Contract Manager.
- Contractors issued with ID Badges from the Estates Helpdesk will only have the minimum level of access for the Trust. Further increased levels of access will need to be formally requested through the Access Control and ID badge Services via the appropriate departmental authoriser who must also supply a time period the access is required for.
- Contractors ID Badges will have a maximum expiry of 12 months as agreed by the Project Manager.

5.7. Access Control and ID Badge Service Responsibilities

- The ID Badge Service is responsible for the issuing of identification badges to all new members of staff on the first day of appointment.
- A central database will be maintained within the Access Control and ID badge Services that will register all names, photographs and details of legitimate staff, official visitors and voluntary staff. The data base will record the following:
 - If the badge is active or not on the electronic control system
 - The date when the badge was activated.
 - The date the badge will expire.

- If the badge has been banned from the electronic control system.
- The levels of access granted to each badge.
- The exact date and time that each badge was last used.
- The exact date and time the badge is used to enter a controlled door.
- Alarms indicating attempts to use the badge on a door without the appropriate access level.

The Security ID Badge will be replaced;

- Every seven years for permanent staff, other expiries will apply for non-permanent staff.
- If the badge is damaged including a damaged image due to the swipe operation.
- If there is significant change to the employee's status.
- If lost and the correct process has been followed. (See 6.2.5 Lost Identity Badge).

6. Standards and Practice

6.1. Door Control

6.1.1. Available Technology

The following technology is available and approved for use with the Trust access control system:

- Hi-Co magnetic stripe incorporated in the Trust ID card.
- Biometric fingerprint recognition.
- Proximity reader incorporated in the Trust ID card.

6.1.2. Entry Control

Doors identified as requiring access control will have card readers and door electronic control mechanisms installed which are activated (opened) by the relevant technology, including the Trust Identity Badge.

6.1.3. Egress (Exit) Control

In most locations egress will be allowed by depressing a green door release button installed as default. An emergency exit control (green 'break-glass' switch) will also be fitted in areas of high sensitivity. Egress will be by a card swipe reader activated by the relevant technology attached to the Trust Identity Badge. Visitor egress to these areas will be by electronic digital code or by remote release controlled by ward department staff.

6.1.4. Fire Alarm Activations

Doors to patient/employee areas will fail safe (open) in the event of fire alarm activations. Doors to certain buildings will fail safe (closed) in the event of fire alarm activation due to their location or sensitivity.

6.1.5. Timed Control of Access

All locations controlled by the electronic control system have the ability to control the locking and release of doors set by automated timed access. Managers can agree a time zone control to suit the requirements of their area.

6.2. Identity Badge

6.2.1 Design

- The standard Identity Badge will be printed on white plastic cards with a Hi-Coercivity magnetic strip embedded on the reverse of the card.
- There will be designated badge designs for all groups of staff and for contractors in this Policy.
- The Access Control and ID badge Services may provide an ID Badge service to other organisations such as SWAST etc.

6.2.2 The Management of Staff ID Badge and Access Levels

Access levels for RCHT employees will be administrated by the Access Control service staff. RCHT personnel will be allowed access to high risk areas only when the Access Control service receives a request from the relevant departmental named authorisers. An up to date list of named authorisers is maintained by the Access Control and ID Badge Services.

6.2.3. The Management of the Contractor ID Badge and Access Levels

- All 'Contracts of Engagement' will contain a clause, which stipulates that the Contractor must, when on site, adhere to the Security and Access Control policies), in respect of ID Badges. A breach of these policies may result in the removal of the offending contractor's employee from the site. Specific contractor's identification badges and access levels will be issued via departmental procedures agreed with the Trust's LSMS and the Access Control Service.
- The Estates Department is responsible for the management and issuing of all contractors ID badges.

6.2.4. Misuse of the Trust ID Badge

The Trust ID badge is issued to an individual member of staff or contractor. The ID badge should not be loaned to another person. Each ID badge creates an audit trail each time it is used on a card reader. The details of every transaction made by an ID badge are recorded by the electronic access control system.

Misuse of a Trust ID badge could lead to disciplinary action being taken against the card holder.

6.2.5. Lost Identity Badge

A lost ID Badge is a potential risk to security until it is reported to the Access Control and ID badge Services staff and rendered inactive. The following course of action should be followed as soon as a badge has been confirmed as lost:

- Prompt reporting of a lost badge is imperative.
- Inform your line manager and the ID Badge Service staff on 01872 25 2260 or via email: rcht.accesscontrol@nhs.net

6.2.6. Visitor Access

For the safety of patients and staff, visitor access to the Trust Hospitals and buildings is only permitted through authorised entrances. Visitors wishing to visit a patient in a ward protected by access control should use the communication system at the ward entrance to announce their visit.

6.2.7. Employees Leaving the Trust

- A list of all staff leaving the Trust will be provided by Cornwall IT Services (CITS) on a weekly basis. All staff listed as leavers will have their ID badge disabled by the Access Control and ID badge Services.
- Line managers are responsible for ensuring that the identification badge is returned to the Access Control and ID badge Services upon termination of a member of staff's employment or, in the case of an official visit, at the end of that visit.
- If a staff member returns to the Trust after retirement, it is their Line manager's responsibility to inform the Access Control and ID badge Services so their card can be reinstated.

6.2.8. End of Contract Periods (Contractors)

- The Estates Department is responsible for the card management of contractors who provide a service to the Estates and Strategic projects and general maintenance of the site.
- Wards or departments who also have management responsibilities for contractors are to ensure that they inform the Access Control and ID Badge Services and Estates Department upon termination/end of the contracted period or work. They are responsible for regaining possession of any card issued to a contractor and returning it.

6.2.9. End of Contract Periods / Internal Move (Staff and Others)

- Wards or departments who have management responsibilities for staff or others issued with a Trust ID card, are to ensure that they inform the Access Control and ID Badge Services upon termination/end of the contracted period or work. They are responsible for regaining possession of any card issued to a member of staff and returning it. Where staff are moving departments then the access control.

6.3. **Purchase of Electric Access Control System**

Care Groups/Departments must consult with the LSMS and the relevant Estates Managers 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).

Equipment purchased must conform to the Trust specification for compatibility with existing systems and be compliant with other statutory regulations and guidance.

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 in the Security folder 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; Communications daily bulletin, all user email, payslip message, screen saver, poster/leaflet.
- 7.4. 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.

8. Monitoring compliance and effectiveness

Information Category	Detail of process and methodology for monitoring compliance
Element to be monitored	The LSMS will ensure that regular audits are carried out on identification badges (ID Badges) and the ID Badge database.
Lead	The Local Security Management Specialist.
Tool	The 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 and the Trust Board. - Externally by the Health and Safety Executive and the Care Quality Commission. Using the Tool (Terminus System).
Frequency	The LSMS will produce an Annual Report for the Director of Estates and Facilities and NHS England on request.

Information Category	Detail of process and methodology for monitoring compliance
Reporting arrangements	Reports are also made to the Health and Safety Committee and Estates and Facilities Performance and Governance Group meetings as appropriate. These meetings will monitor the implementation of this policy in terms of effectiveness and performance by reviewing incidents and Datix reports and report to the Trust Board.
Acting on recommendations and Lead(s)	The 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 require action will be taken to the Estates and Facilities Performance and Governance Group.

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. 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:	Access Control Policy V3.0
This document replaces (exact title of previous version):	Access Control Policy V2.0
Date Issued/Approved:	December 2024
Date Valid From:	December 2024
Date Valid To:	December 2027
Author/Owner:	Natasha Quick, Acting Head of Security / LSMS.
Contact details:	01872 25 2147
Brief summary of contents:	Security Policy, Identity Badge, Reporting Security Incidents, Purchase of Security Systems, Reporting Security Incidents, Site Security, Building Security, Personal Security of Staff, Identification of Personnel, Visitor Access, CCTV, Purchase of Security Equipment.
Suggested Keywords:	Access Control Policy, Security Policy, Identity Badge, 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.
Manager confirming approval processes:	Natasha Quick, Acting Head of Security.
Name of Governance Lead confirming approval by speciality and care group meetings	Debbie Price, Business and Security Systems Manager.

Links to key external standards:	The standards for providers security management.
Related Documents:	Guide to good practice for the Security of Premises. Security Identity Badge Protocol. Procedure for the Reporting of all Criminal and Security Incidents. Lone Working Policy
Training Need Identified:	Yes, the Learning and Development department have been informed.
Publication Location (refer to Policy on Policies – Approvals and Ratification):	Intranet Only
Document Library Folder/Sub Folder:	Estates and Facilities /Security.

Version Control Table

Date	Version Number	Summary of Changes	Changes Made by
Jan 2014	V1.0	Policy written.	Paul Dixon Security Manager / LSMS
Oct 2016	V1.1	Reviewed and updated.	Paul Dixon Security Manger / LSMS
March 2021	V2.0	Full three-year review and changed to the reporting structure/standards.	Paul Dixon Security Manager / LSMS
Sept 2024	V3.0	Full three-year review and changes to reporting structure/name and responsibility changes.	Natasha Quick, 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
rcht.inclusion@nhs.net

Information Category	Detailed Information
Name of the strategy/policy/proposal/service function to be assessed:	Access Control Policy V3.0
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):	Natasha Quick, LSMS.
Contact details:	01872 25 2147

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 access control 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?	ID badge and access control database audits.
5. Who is intended to benefit from the policy?	All Staff.

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: All attendees of the Health and Safety Committee. Health and Safety Leadership Team.
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 discriminate with any religious or cultural beliefs.
Marriage and civil partnership	No	This Policy does not impact on marriage/ civil partnership.

Protected Characteristic	(Yes or No)	Rationale
Pregnancy and maternity	No	This Policy does not impact on pregnancy/ 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](#)