

Document Control

Title Security Identification Badges Standard Operating Procedure			
Author		Author's job title Fire & Security Advisor	
Directorate Facilities		Department Estates	
Version	Date Issued	Status	Comment / Changes / Approval
0.1	Mar 14	Draft	Initial version for consultation
1.0	Apr 14	Final	Approved by Facilities for publishing on Bob
1.1	Oct 15	Final	Amendment to ID badge request form
2.1	May 16	Revision	Revised some incorrect wording
2.2	July 16	Revision	Revised to include reference to the Trusts "Leavers Policy."
3.0	June 17	FINAL	Three year policy review
4.0	May 19	Draft	Review due to significant expansion of system.
4.1	Feb 20	Revision	Revised contacts & governance structure
4.2	Sept 20	Revision	Revised contact at 3.3
4.3	Feb 21	Revision	Addition of Secure Access System on Residences & updated Appendix A
Main Contact Fire, Security & Technical Services Officer Facilities Department North Devon District Hospital Raleigh Park Barnstaple, EX31 4JB		Tel: Direct Dial – Tel: Internal – Email:	
Lead Director Divisional Director of Facilities			
Document Class Standard Operating Procedure		Target Audience All staff	
Distribution List		Distribution Method Trust's internal website - BOB	
Superseded Documents Security Identity Badge Policy v3.0			
Issue Date February 2021		Review Date May 2022	Review Cycle Three years
Consulted with the following stakeholders: (list all) <ul style="list-style-type: none"> HR/Medical Staffing Facilities Administration Team Local Security Management Specialist and Health & Safety Manager Legal Claims Manager 		Contact responsible for implementation and monitoring compliance: Fire, Security & Technical Services Officer	
		Education/ training will be provided by: N/A	
Approval and Review Process <ul style="list-style-type: none"> Head of Estates 			

Local Archive Reference

G:\Facilities\Facilities Procedural Documents\BOB\Archive

Local Path

G:\FACILITIES PROCEDURAL DOCUMENTS\BOB

FilenameG:\FACILITIES PROCEDURAL DOCUMENTS\BOB\SOP Security Identity Badge V4.1
2020February.docx**Policy categories for Trust's internal website (Bob)**

Security, Facilities

Tags for Trust's internal website (Bob)Badges, Security, ID, secure access, swipe
access, access permission**Any revision to an NHSLA document requires the agreement of the Senior
Governance Manager (Compliance)**

CONTENTS

Document Control	1
1. Introduction	4
2. Responsibilities	4
Management Responsibilities	4
Staff Responsibilities	4
Human Resources Department Responsibilities	5
Facilities Department Responsibilities.....	5
3. New ID Badge/New Access Permission	6
4. Lost/Stolen ID Badge	6
5. Expired ID Badges (Inactivity)	6
6. Lock Out Procedure	6
Damaged ID	6
Accidental Lock Out.....	7
24 hour departments.....	7
Closed Departments	7
7. End of Service/Leaving the Trust	7
8. Short Term / Non-Staff ID	7
Medical/Clinical.....	7
Work Experience/Shadowing	8
Contractors	8
Voluntary Organisations.....	8
External Partner Agencies	8
9. Enforcement	9
10. Education and Training	9
11. Monitoring	9

1. Introduction

- 1.1. Security is an integral part of patient care and an identification badge (ID) complete with the facility for electronic access to areas is a key element in providing a safe, secure environment.
- 1.2. It is vital to be able to identify and recognise fellow staff and individuals with a bona fide reason for being on the premises. This can be achieved by ensuring that all staff wear ID.
- 1.3. Any outside agencies requiring access to Trust's premises in the course of their official duties must also adhere to the Trust's Secure Environment Policy. This includes the procedure for obtaining satisfactory Identification.
- 1.4. Trust supplied ID Badges can also be programmed providing secure access to areas local authorisation is required. This Standard Operating Procedure (SOP) relates to all staff, contractors, volunteers and external agencies.

2. Responsibilities

Management Responsibilities

- 2.1. Managers are responsible for ensuring that all staff are aware of the Trust's Secure Environment Policy and that ID is worn and clearly visible.
- 2.2. The line manager is responsible for ensuring that ID is returned upon termination of staff's employment.
- 2.3. Managers must ensure that arrangements are in place for providing ID for official visitors or contractors working in their areas of responsibility as instructed within the Secure Environment Policy.
- 2.4. Managers are responsible for monitoring the implementation and compliance with Secure Environment Policy and this SOP.

Staff Responsibilities

- 2.5. All staff are to ensure that ID is worn at all times and that it is kept secure when not being worn. ID must be worn in the holder provided and displayed in a prominent position at all times.
- 2.6. Where staff have access permission to a secure area (see Appendix A) they must ensure their ID remains active by swiping their card against a reader at least once every 60 days.
 - To ease the task of remembering to do so it is advised staff swipe their ID on a reader weekly. Staff can use any reader even if the door is unlocked/open.
- 2.7. ID must only be used by the staff member that it is issued to and named on the ID; as access rights differ on an individual case by case basis.

- 2.8. All staff must report lost or damaged ID on the Trusts incident reporting system (DATIX). It is recognised that it may not be appropriate for some clinical staff working in controlled areas, i.e. Theatres, to wear ID. Once staff exit the controlled area then ID badges must be displayed.
- 2.9. All staff are expected to challenge anyone not displaying appropriate ID where it is safe to do so.
- 2.10. Where staff witness suspicious activity or persons not wearing ID appropriately and it is considered unsafe to approach, the situation must be reported and escalated to site management and security officers without delay.

Human Resources Department Responsibilities

- 2.11. A central ID database will be maintained by the HR Team. This will register all names, photographs and details of employees and voluntary staff.
- 2.12. The HR Department will replace ID if:
- ID is damaged or mislaid
 - There is significant change to the employee's status.
- 2.13. The HR Department will email the Facilities Department with the access granted by the relevant site/area/department manager.
- 2.14. The HR team are responsible for issuing the leavers list to Facilities which will result in any access rights being removed from ID (Ref: Leavers Policy).

Facilities Department Responsibilities

- 2.15. The Facilities Department will programme ID badges with the permitted access (refer to appendix A).
- **This will be carried out on Wednesday afternoons & Friday afternoons between 14.00-16.00hrs.**
- 2.16. The Fire and Security Advisor with the department managers will carry out regular security checks on ID.
- 2.17. The Facilities Department will monitor and upkeep the computerised secure access system including a database of staff:
- Full Name
 - Gender
 - Department/Area of employment i.e. Estates/Ward etc.
 - Access level
 - Card status and actions
 - Expiry (if required)
 - Notes
- 2.18. Estates supervisors will report any access cards not returned by day contractors for deactivation.

3. New ID Badge/New Access Permission

- 3.1. On commencement of employment all members of staff will be issued with a Trust ID to be used in accordance with Staff Responsibilities 2.5 to 2.10 inclusive. This should be issued by managers at induction.
- 3.2. Any volunteer agencies will collect their ID from the Human Resources (HR) Department.
- 3.3. Requesting new access permission should be performed by email with justification to the department manager as indicated in Appendix A. If access is approved email proof should be forwarded to the system's principal administrator lucy.trimm@nhs.net

4. Lost/Stolen ID Badge

- 4.1. Lost or stolen ID badges must be reported via DATIX.
- 4.2. For sensitive secure areas (Theatres, Maternity, Mortuary etc.) staff and managers should additionally make contact with the Fire and Security Advisor to expedite security access being suspended as soon as the loss/theft is noticed. Should the card be found this can be reinstated in person as per 5.2.
- 4.3. Replacement badges must be ordered through HR. These will automatically be sent to Facilities in order to be loaded with the required access prior to being issued.

5. Expired ID Badges (Inactivity)

- 5.1. Access will automatically expire on all issued ID badges after 60 days of inactivity. Typically this is due to extended periods of leave or absence from work. Alternatively it may be due to staff members regularly tailgating or infrequently visit secure areas or failing to swipe their ID badge as per 2.6.
- 5.2. Staff may request reactivation through the facilities helpdesk which is open Monday-Friday 0800-16.30. **This request must be in person in order to confirm staff identity.**
- 5.3. The ID must be swiped on the day of reactivation otherwise it will revert to an inactive state the following day.

6. Lock Out Procedure

Damaged ID

- 6.1. Where an ID badge becomes damaged, defaced or worn it does not form part of the secure access system and should be replaced immediately.

- 6.2. If a card fails to give access to a door that staff are authorised to use (and has been applied to the card) staff should inspect the card closely for damage: cracked, bent or deformed cards may have damaged the internal contactless technology. Contact HR for a replacement. For short term emergency access whilst a replacement is produced: follow the accidental lock out procedure.

Accidental Lock Out

- 6.3. Accidental or inadvertent lock out can occur where an ID Badge has been left inside a secured area and the staff member leaves the secure area. This would be no different to getting locked out at home, embarrassing, but readily resolved.

24 hour departments

- 6.4. Where the department is manned 24 hours the staff without ID may be allowed back in by the staff inside – assuming that the locked out staff are recognised and access is required. **If in doubt, do not permit access.** Means by which locked out staff can alert the staff inside in vary, dependant on location: Intercom, internal telephones, door bells or simply knocking on the door.

Closed Departments

- 6.5. Staff that accidentally or inadvertently lock themselves out of an unmanned secure department (or if unable to contact staff inside a 24 hour department) should contact site management to assist gaining access.
- 6.6. At NDDH Clinical Site Managers (Bleep 500) can provide escorted access to all secure areas. Staff should either contact Bleep 500 direct or contact Switchboard to assist in contacting Bleep 500. **Staff must recognise the inconvenience of being locked out of your department will be prioritised along-side the clinical needs of the Trust.** Be patient.

7. End of Service/Leaving the Trust.

- 7.1. All ID must be returned to the Trust in order to be appropriately disposed of.
- 7.2. For sensitive secure areas managers should additionally make contact with Facilities to expedite security access being suspended as soon as staff leave the Trust.

8. Short Term / Non-Staff ID

Medical/Clinical

- 8.1. Short-stay locum medical staff will be issued with a temporary ID. ID will only be issued on proof of identity. The temporary ID will expire on the last day of service.

Work Experience/Shadowing

- 8.2. Work Experience students following a programme will be issued individual ID showing their name and attached department prior to starting with the trust. This ID will not be programmable with security access.
- 8.3. In order for individuals to prove ID whilst on a formal Work Shadowing placement will be issued with a Trust ID stating “work shadowing” as name and job title. This ID will not be programmed with security access.
- 8.4. Individuals on either Work Experience or Shadowing are to be allowed access to secure areas by the members of staff which they are shadowing. Those staff are responsible for the individual.

Contractors

- 8.5. The Estates Management Teams will issue all contractors with a site safety leaflet (code of conduct) to ensure compliance with the Contractors Policy. Facilities Contractors and official visitors will collect ID from the Facilities reception.
- 8.6. Access cards for long term contractors will be a blank style card but will be programmed with minimum required access as per a Trust ID badge.
- 8.7. Day contractors will be issued with a numbered blank style access card which will be signed out by contractor as if it were a key. This must be returned at the end of the working day; any cards not returned on the day of issue will have all access revoked.
- 8.8. If an access card is lost/not returned the contractor/company will be liable for the cost of a replacement card. The charge for a replacement card will be £5.00 Inc. VAT.
- 8.9. The Trust will not seek recover costs for cards that have been returned and have become damaged through normal wear and tear.

Voluntary Organisations

- 8.10. Voluntary organisations/volunteers that support the Trust on a regular basis will have Trust ID. Volunteer ID must be displayed at all times.

External Partner Agencies

- 8.11. Staff belonging to external agencies, (e.g. SWAST, Patientline, CQC Inspectors etc.) will be required to wear their own organisation’s ID. ID must be worn at all times when on Trust premises and be clearly visible.

9. Residence Secure Access System

- 9.1. The residences blocks are secured by a similar but separate secure access system to the main building which is administrated by the Sodexo Residences team.
- 9.2. The Residences have an additional layer of security in the form of facial recognition, minimising the likelihood of staff being locked out or requiring their Staff ID out of hours.
- 9.3. Staff will be enrolled on to the residences system as part of the checking in process. Their information will be stored securely and will only be retained in line with GDPR.

10. Enforcement

- 10.1. Patients, contractors and visitors must be assured that when they enter the Trust's sites they are entering a safe and secure environment. All users must have confidence that the system will keep them secure and that staff are there to help.
- 10.2. The Trust will publish and signpost the fact that a security ID system is in use and that visitors can expect to be challenged.
- 10.3. Breach of the Secure Environment Policy, Leavers Policy and this SOP could result in disciplinary action.

11. Education and Training

- 11.1. The Trust Fire and Security Advisor is responsible for communicating this procedure, via the Trust Intranet.

12. Monitoring

- 12.1. The Trust's Fire and Security Advisor is responsible for random monitoring of compliance with this procedure. Routine checking of permitted access reviewing the ID badge SOP.


APPENDIX A: LIST OF AUTHORISING PERSONS

Department	Authoring Persons
A&E	Lisa Wells / Jo Hope
CCTV Security Suite	Dave Macbeth / Steve Gladwin
Estates Workshop & Plant rooms	Luke Green
External Doors (Lockdown)	Dave Macbeth / Luke Green
Fern Centre	Tasmin Andrew / Dawn Gray
Finance Department	Colin Dart / Nina Phillips / Karen Sandwell
Healthcare Records	Janet Hillman / Pat Anton / Sharon Griffin
IT Workshop & Server Rooms	Geoff Smith / Paul Mitchell
Level 00 Ladywell Link Corridor	Jonny Morgan / Dave Macbeth
Level 00 Service corridor	Darren Proctor / Dave Macbeth
Male Cyclist Changing Area	Charlotte Richardson / Lucy Trimm
Medical Education Centre (MEC)	Caroline Rawlings
Mental Health Inpatient Wards (Ocean, Moorland and Meadow View)	Jody Lapinskas (Ocean View) / Pdraig Doherty (Meadow View) / Laura Barrie (Moorland View)
Mortuary	Lee Luscombe
Pathology	Tim Watts / Annette West
Pharmacy	Pam Outram / Matt Kaye
Physiotherapy	Darren West / Victoria Typaldou / Helen Cooke
Pre-Op / Booked Admissions	Debbie Ludwell
Rheumatology/EEG/EMG	Lyndsey Stanbury
Seamoor Unit	Shantelle Buckingham / Dawn Gray
Switchboard & ISDX Room	Carol Smart / Sarah Patton
Theatres/Day Care Theatres/Theatre 7	Andy Martin / Maureen Rotherey
Trinity Suite	Anne Flory / Jackie Woodward /Paula Howells
Wards	
Level 1: Acute Medical Unit (MAU& GP Referral) & Alex Ward	No authorisation required
Level 3: Capener, Lundy, Tarka	No authorisation required
Level 4: Fortescue, KGV, Victoria	No authorisation required
Level 5: Glossop, Staples	No authorisation required
Caroline Thorpe Ward	Jonny Morgan / Joanne Hayward / Anita Chin
Maternity (Delivery Suite & Basset Ward)	Jonny Morgan / Joanne Hayward
SCBU	Jonny Morgan / Ade Agoro /Claire Walker
Community Sites	
Bideford Community Hospital	Andrea Small
Hugh Squire Ward (South Molton)	Karen Partridge
Sexual Health Clinic (Barnstaple Health	Jayne Lacey

Centre)	
---------	--

APPENDIX B: INTERNAL HEALTH AND SAFETY ALERT.
ALERT 13: DRIVIN WHILST WEARING LANYARDS. DATE: 29.03.19

Classification of Alert		Distribution and Action
Immediate Action	x	1. All Staff, Trust wide
Acton	Cascade	
Update		

Equipment	
	<p>Dangers associated with driving whilst wearing lanyards.</p>
Problem	
<p>A safety warning recently issued by Dorset Police is being shared following two road traffic accidents where injuries have been exacerbated by the wearing of lanyards with ID badges.</p> <p>The Police are urging drivers not to wear lanyards whilst driving. One driver was involved in a minor road traffic accident whilst wearing a lanyard and ID badge. The driver’s airbag triggered with force which caused the ID badge to be pushed into the driver’s chest resulting in a collapsed lung. Had the driver not been wearing their lanyard it is likely they would have walked away from the incident rather than requiring hospital treatment.</p> <p>In another incident, an NHS worker had keys attached to their lanyard. Whilst driving home she was involved in a road traffic accident. The crash triggered the driver’s airbag causing the keys to be pushed into her body which then perforated her bowel. This resulted in hospital treatment for more than six weeks.</p> <p>Advice from the Police is to remove lanyards and ID badges when leaving the office for “safety and security” reasons especially when driving. Use of lanyards with breakpoints is also advised.</p>	
Action	
<ul style="list-style-type: none"> • Whilst driving (or being a passenger in a vehicle) do not wear lanyards or similar objects around the neck with ID badges, sets of keys and the like, taking note of the learning and advice provided by the Police. • Lanyards with three break points are recommended for use by all staff. • Further general information regarding driving, lone working & personal safety is provided on BOB. • The Carrying Equipment and Transporting Patients In Cars Guidelines have recently been reviewed and updated and cover the use of trust owned pool cars, hire cars and private vehicles. 	
Alert issued by	Mike Cousins Health and Safety Manager
For further information	Mike Cousins, Health and Safety Manager. 01271 311 725 Health and Safety intranet pages (BOB)