South East Coast Ambulance Service NHS
NHS Foundation Trust

ID & Access Procedure

Contents

1 Scope

1.1. This procedural document, and the Security Management Policy it pertains to, exists to set out specific protocols for the management of ID & access security within South East Coast Ambulance Service NHS Foundation Trust (the Trust).

1.2. By ensuring a robust culture combined with effective monitoring, Trust Staff, Contractors, Volunteers, visitors, patients will be better protected against such aspects as violence/aggression, false representation and unauthorised access. This in turn will assist in the protection of Trust vehicles, equipment, and premises from such crimes as theft and criminal damage.

1.3. This document will define the correct processes in relation to the management of requests for cards, access rights, challenging, accountability, incident reporting and investigations.

2 ID Cards and Permissions

2.1. ID cards are an important form of identification to demonstrate eligibility to perform duties for the Trust, cover safety and security for staff and patients and to grant access to areas with access control. Cards must always be kept on the person (and where possible worn/displayed) whilst performing duties for the Trust, whether on or off Trust sites.

2.2. All employees are required to hold a valid and up to date ID card whilst performing duties within the Trust. Requests for access rights, new or replacement ID or ID access cards or must be submitted with the required information.

2.2.1 Current name, which must match HR records (not use a known as)
2.2.2 Preferred pronouns
2.2.3 Up to date professional picture (not as stringent as passport)
2.2.4 Job title (substantive role)
2.2.5 Access requirements (only for duties)

2.3. There may be circumstances where alternative arrangements are implemented to manage ID security with functionality. Matters arising must be escalated to the Health, Safety & Security team for initial review and onward consideration.

2.4. Cards are be produced centrally at main offices and is the responsibility of the receptions or locally in Operating Units where authorised by the Security Manager however permissions, activation, expiry etc. may only be carried out by the Health, Safety & Security team overseen by the

Security Manager/Head of Health, Safety & Security has authorised another individual.

2.5. Where local Operating Units produce cards, any expenses such as equipment, inks, blank cards etc. whilst are the responsibility of the local Operating Unit, order requirements should be put through NeedID@Secamb.nhs.uk to ensure appropriate auditing of quotes and orders is monitored.

2.6. ID Cards are produced with a receipt the named individual on the card must personally sign to confirm they will adhere to use the card appropriately and within relevant governance and legislation. The signed receipt must be returned by one of the mechanisms listed on the receipt for cards which have access capability for associated permissions to be activated.

2.7. Access permissions are assigned and activated centrally within Health, Safety & Security and will be determined by the role and routine duties carried out. Additional permissions may be granted indefinitely or for a defined period should the duties require. A request should be made to NeedID@Secamb.nhs.uk which is authorised by a line manager for the staff member.

2.8. All contractors, maintenance staff and sales representatives, etc. that come onto Trust premises must wear an appropriate identification badge. Contractors on the Trust site must make themselves aware to the site reception, Estates Department or Maintenance Department as appropriate and obtain a “Visitors” badge.

2.9. Duties for some individual groups and or companies may require/allow for Trust ID cards to be produced. In such instances there must be appropriate governance arrangements and legal protection with the NHS Employers Checks as covering Trust employees being consistently applied for these individuals or companies for those working around staff, vehicles, equipment, medicines, and controlled drugs. Assurance must be provided to the Trust representative for the individual group or company that these checks have been completed with no concerns. The NHS Employers checks include as required;

- References – to cover the last 3 years
- ID check
- Right to work check
- Occupational Health Check
- Professional registration and qualification checks
- DBS check (if applicable)

2.10. All other visitors must sign in at the Main Reception and obtain a “Visitors” or “Contractors” badge as appropriate and signed out on completion.

2.11. Temporary or agency staff may be considered for an ID card if their period of work is three months or more. Local management should conform with existing local arrangements with any queries directed to the Security Coordinator.

2.12. All employees should be prepared to be challenged, by any other employee of any level whether in civilian clothing, office attire or uniform, if they are not recognised, to produce their ID card.

2.13. ID cards must never be loaned to another individual, used for an inappropriate purpose, treated negligently or recklessly leading to damage/loss. To do so would be a breach of the signed agreement (receipt) and may constitute a breach of security. Incidents of such a nature must be reported through and investigated by the line manager. Depending on the type and level of breach, this may result in a warning and/or capability/disciplinary proceedings.

2.14. Loss or theft of an ID card must be reported via an IWR-1 and emailed NeedID@Secamb.nhs.uk) so permissions can be suspended. Loss or theft will not usually incur proceedings unless through investigation it is deemed to have occurred due to a breach of security as described above.

2.15. Redundant or expired ID cards must be securely destroyed. Where an employee is leaving the Trust, the card must be returned to their line Manager on the day they leave for secure destruction.

3 Site Access

3.1. The Trust operates a range of access measures from manual locks to keypads to swipe card access control. It is vitally important for governance and security that the associated access means, i.e. keys, codes or ID cards are held and disseminated securely by all employees to prevent breaches of governance and security which may threaten the safety and security of employees.

3.2. Site access is a part of both the security audit process (see associated procedure) and Security Management Strategy (see associated document) to build a robust culture to ensure all employees are aware of their duties to protect themselves and their colleagues.

3.3. Unknown persons, including employees, tailgating or shadowing into or out of swipe access controlled areas must not occur and should be challenged by employees witnessing this for the staff member to swipe or if they do not have an ID card, report to reception to sign in.

3.4. Any employee is responsible for security where they allow a visitor or contractor access and must ensure the individual has signed in appropriately, is expected (this may be check by reception if a main

office) and ensure the individual does not move through the site unescorted even if confirmed as expected.

3.5. Where an individual is expected and waiting in a reception area, it is the duty of the expecting employee/manager to collect or appoint a colleague or member of their team to collect and escort the visitor/contractor.

4 Responsibilities

4.1. **Chief Executive**

4.1.1. Ultimately responsible for all policies and procedures within the Trust, including those pertaining appropriately maintaining secure access arrangements to protect Trust staff, property and assets.

4.2. **Security Management Director (SMD)**

4.2.1. Responsible for ensuring processes, procedures and systems are in place to manage security access arrangements to protect Trust staff, property and assets.

4.3. **Non-Executive Security Director**

4.3.1. Responsible for ensuring that the business of the Trust does not compromise the requirements and directions issued by the Secretary of State, the Department of Health and NHS England relating to security.

4.3.2. **Head of Health, Safety & Security**

4.3.3. Responsible for planning and, following Exec/SMD approval, implementing the strategic direction for access and security of Trust sites.

4.4. **Security Manager**

4.4.1. Responsible for the management of the overarching ID card process, the Trust access system, access levels and rights appropriate for managers and staff to fulfil their duties.

4.5. **Security Coordinator**

4.5.1. Responsible for administration of the Trust access system, handling access requests and enquiries and coordinating security matters relating to access/permissions.

4.5.2. Responsible to produce specialist ID cards not authorised to be produced locally by receptions or OUs including, unnamed, generic, contractor and/or site master cards.

4.6. **Managers**

4.6.1. Responsible for ensuring staff comply with necessary processes for card requests and access rights.

4.6.2. Ensuring local operating areas work to a robust culture of appropriate usage, storage, display and updating of ID cards and appropriate access for local sites, staff challenges and routine monitoring of staff through site and where necessary, sport checks.

4.6.3. For OUs with printing capability a suitable Manager should be identified for the oversight of OU card production. For centralised services reception cover the management of card production under the process in this procedure.

4.6.4. Responsible for ensuring ID cards for leavers are collected or handed in and securely disposed of.

4.6.5. Notifying NeedID@Secamb.nhs.uk of any leaver so the permissions can be withdrawn.

4.6.6. Where incidents occur such as loss, theft, false representation, unauthorised entry, trespass etc.; responsible for ensuring that the incident is recorded and reported via an IWR-1 with an internal manager's investigation is conducted.

4.6.7. If individuals refuse to return their ID card, Managers will ensure written correspondence through HR and leavers/termination confirms ID cards are to be returned and to communicate to the individual on a minimum of two occasions in writing within four week period, of the requirement to return. If this is not met a seven-day warning letter can be sent that the matter will be pursued by the Manager with the Police and followed up if the individual still refuses to comply.

4.7. **All Employees**

4.7.1. Responsible for following the appropriate process for a new or replacement ID card as per this procedure. Access will only be granted for appropriate doors to assist in completion of routine duties.

4.7.2. It is the responsibility of the individual to ensure their details are up to date and to request a new card should details change or the card expire. Individuals may request a new ID card up to four weeks before the card's expiry date.

4.7.3. Must follow the appropriate ID & Access responsibilities guidance (Appendix B) for card and access usage, ensuring employee and access security whilst operating within or across sites which use a swipe card, keypad, manual lock (or combination of).

4.7.4. For OUs with card production capability, a suitable representative in administration should be tasked with card production or centralised services receptions are responsible for named individual card production. For Community First Responders a suitable Trust representative in the support department should be nominated to produce ID cards.

4.7.5. Those in the process of applying for a card, have lost or had stolen a card or where the site has no swipe access point are required to sign in on arrival and out when leaving and where available collect a temporary pass to be handed back to reception when leaving.

4.7.6. Responsible for taking ownership of personal and Trust security in line with Trust values and the Security Management Strategy (see associated document).

4.7.7. Ensuring when leaving the Trust that cards are returned to the appropriate line Manager.

4.7.8. Responsible for reporting incidents on the appropriate form (IWR-1) for instances including but not limited to;

4.7.7.1 Loss or theft of a card (must also email NeedID@Secamb.nhs.uk) so permissions can be suspended.
4.7.7.2 Trespass or unauthorised access to sites or secure areas within sites by non-Trust employees.
4.7.7.3 Concerns of false representation by non-Trust employees.
4.7.7.4 Violence and/or aggression experienced from non-Trust employees accessing any part of a site where unauthorised.

5 Audit and Review

5.1. The Security Manager will continuously monitor the content through its use, to ensure it meets the security needs of the Trust, whilst remaining relevant and appropriate prior to its scheduled review.

5.2. The procedure will be reviewed every three years or sooner if new legislation, codes of practice or national standards are introduced.

6 References

6.1. The Department of Health and Counter Fraud Security Management Service – A professional approach to managing security in the NHS
6.2. Health and Safety at Work Act (1974)
6.3. Criminal Justice Act (1988)
6.4. NHS Protect Security Management Standards

South East Coast Ambulance Service NHS
NHS Foundation Trust

Appendix A: ID (Inc. access) Card Receipt Template

South East Coast Ambulance Service NHS
NHS Foundation Trust

Return this form to either:

1. The address opposite
2. Scan/email to NeedID@secamb.nhs.uk

Your card will not be activated until this form has been received

ID Card Receipt
Security Coordinator
SECAMB
Heath Road
Coxheath
Kent
ME17 4BG

Provision of Trust Identity Card

As a SECAMB employee, a signature is required upon provision of a new Trust Identity card, which is issued under the following conditions.

The card remains the property of the Trust and must be returned upon termination of employment. The safekeeping and appropriate use of the card is the responsibility of the person that it is issued to. ***It must not, under any circumstances, be given to or used by anyone else.*** The card may be treated as proof of employment and, where appropriate, as a means for allowing access to Trust buildings. The card must remain on your person whilst performing your duties as a Trust employee and should be kept secure (preferably at home) at all other times, where possible ID cards should be worn/displayed.

On receiving this form and your card diarise the card expiry 1 month prior to the date listed to allow time to request and receive a replacement card as permissions will automatically cease following expiry.

If the card is lost of stolen, it is to be reported immediately via the Trust Incident reporting system (Datix) and to immediate notify NeedID@secamb.nhs.uk – who will then deactivate the card to avoid it being used by any unauthorised persons.

Please sign below to accept the card and to confirm you have read and agree to the terms above and you will adhere to the **ID & Access procedure** (Which can be found on the Trust Intranet). Lastly, sign the cardholders strip on the rear of the card and record the eight-digit number found on the front of the ID card below, before returning the form.

This card replaces card No ..... *N/a* ☐

Reason for new card issue: New request ✓☐ Lost card ☐Change in Name Details☐
Change in Job Role ☐ Card Expired ☐

Print name: .....

Location/Department: .....

Card no: .....

Job title: .....

Signature: .....

Date: ____/____/_____

South East Coast Ambulance Service NHS
NHS Foundation Trust

Appendix D: Guidance Reminder

1. Requests for new /replacement cards should be sent to NeedID@Secamb.nhs.uk and where applicable include;

    - Current name, which must match HR records (not use a known as)
    - Up to date professional picture (not as stringent as passport)
    - Job title (substantive role)
    - Access requirements (only for duties)

2. Card production may be carried out in OUs, main offices or 111 by anyone who has completed the appropriate card production form. Activation and permissions are only authorised centrally within Security unless specifically authorised by the Security Manager with the appropriate activation/permissions form.

3. New, additional or changes to access/permission requirements should be emailed to NeedID@SECAmb.nhs.uk confirming their relevance to role/duties and evidencing that a senior manager has approved the request.

4. All individuals must adhere to use the ID card appropriately and within relevant governance and legislation. Misuse, multiple losses, loaning a card etc. may constitute a breach of security.

5. All individuals should only be in possession of one SECAmb ID card at a time, redundant cards must be securely destroyed.

6. Staff should feel comfortable to challenge others for ID where they do not recognise the person, whether in office attire, uniform, or casual dress. In turn staff should be prepared to be challenged themselves for ID.

7. Concerns on false representation, trespass or violence/aggression from non-Trust employees following unauthorised access must be reported as an IWR1.

8. NeedID@Secamb.nhs.uk must be informed so permissions applied to ID cards can be frozen where there is loss or theft of an ID card (as well as completing an IWR-1)

9. NeedID@Secamb.nhs.uk must be informed where a security risk exists due to an individual leaving under disputed circumstances or AWOL etc. and their ID card is still in their possession.

10. All staff are responsible for their own and their colleague's safety and security and so must not allow unknown persons tailgating, should challenge for ID and ensure visitors report to reception to be confirmed as expected by the relevant person/department.