Ashford and St. Peter's Hospitals
NHS Foundation Trust

# Registration Authority (RA) Policy

**Author:** **Nicki Rayment – Head of Digital Programme Delivery**

**Executive Lead:** **Simon Marshall – Director of Finance**

**Status:** Approval date: July 2021

Ratified by: Information Governance Steering Group

Review date: July 2024

Patients first • Personal responsibility • Passion for excellence • Pride in our team

**History**

| Issue | Date Issued | Brief Summary of Change | Approved by |
|---|---|---|---|
| 1 | February 2012 | New policy | IGSG |
| 2 | February 2015 | Document reviewed and revised in the light of changes to national governance. | IGSG |
| 3 | August 2021 | Rewrite of previous policy | IGSG (Chair's action) |

| For more information on the status of this document, please contact: | |
|---|---|
| Policy Author | Nicki Rayment - Head of Digital Programme Delivery (RA Manager) |
| Department/Directorate | Digital Services |
| Date of issue | July 2021 |
| Review due | July 2024 |
| Ratified by | Information Governance Steering Group |
| Audience | All staff and non-ASPH staff using Smartcards, including those from any defined child organisation |

## Executive summary

The local Registration Authority (RA) ensures that individuals providing healthcare services to the NHS directly, or indirectly, have access to NHS Spine connected applications and information in accordance with their role. It is the Trusts' responsibility to ensure that the requirements of the RA is met and maintained, to adhere to the NHS Confidentiality Code of Practice and the NHS Care Records Guarantee.

The purpose of this document is to outline the agreed responsibilities and processes required (including any emergency processes required as part of the response to a major incident) to support the implementation of the local registration authority including the Electronic Staff Record (ESR) Interface and Care Identity Service (CIS) across the Trust.

## Contents

**SECTION** **Page**

### Appendices

**See also:**

- Information Governance Standard Operating Procedure No.4 – User Access Management
- Registration Authority Standard Operating Procedure No.1 - Access Control Position Management
- Registration Authority Standard Operating Procedure No.2 – Annual Review of Spine Positions
- Registration Authority Standard Operating Procedure No.3 – Child Organisation Process
- Incident Reporting and Management Policy

# 1. Introduction

Ashford and St Peter's Hospitals NHS Foundation Trust (ASPH) is a local Registration Authority (RA) authorised to carry out on behalf of the NHS the registration of individuals and issuance of NHS Smartcards.

The local RA ensures that individuals providing healthcare services to the NHS directly, or indirectly, have access to NHS Spine connected applications and information in accordance with their role. It is the Trusts' responsibility to ensure that the requirements of RAs are met and maintained, to adhere to the NHS Confidentiality Code of Practice and the NHS Care Records Guarantee.

From April 2008, NHS Employment Check Standards became a requirement in the NHS as part of the annual health check. Similarly, robust identity checks were also enforced using the same identity management standards carried out by an NHS Registration Authority (RA) to verify an individual's identity before allowing access to Spine connected applications. Combining these two parallel activities into a single Integrated Identity Management (IIM) process has proven to deliver significant benefits through HR/RA Process Integration and the move to Position Based Access Control (PBAC).

Integrated Identity Management significantly improves access control to Spine connected applications containing person identifiable information through revised business processes and the introduction of new software applications.

Based on the significant benefits and improved governance, ASPH has implemented the integrated PBAC through the Electronic Staff Record (ESR) interface alongside Care Identity Service (CIS).

Failure to adhere to this Policy, for Smartcard users and administrators, constitutes a breach of employment Terms and Conditions and could result in disciplinary action or removal of Smartcard access.

# 2. Scope

This document is the Registration Authority (RA) Policy for the Trust, and RA child organisation; it is relevant to both Registration Authority and ESR users to ensure that any changes made in ESR or CIS, particularly during a major incident, are considered and reviewed in accordance with the continued functionality of the software and the National Registration Authority Policy[1]

[1] https://digital.nhs.uk/services/registration-authorities-and-smartcards#national-registration-authority-policy

## 3. Purpose

The purpose of this document is to outline the agreed responsibilities and processes required (including any emergency processes required as part of the response to a major incident) to support the implementation of the local registration authority including the ESR Interface and CIS across the Trust.

The document is not intended to be an exhaustive review of all HR and RA processes and procedures but rather will focus on necessary changes to the following key elements:

- new starter setup (from acceptance of offer to employment)
- non-ASPH employed individuals
- managing changes to a person’s details, assignments and positions
- leaver’s process
- access control

## 4. Explanation of Terms Used

**Access Control Position (ACP)** – provide a simple and effective mechanism for providing users with the access they need in the course of their work.

**Advanced RA Agent** – Has the ability to action nearly all of the RA processes available to the RA Manager except the ability to assign users to RA roles in their own organisation and assign RA Managers in child organisations that are RA hosting.

**Care Identity Service (CIS)** – Care Identity Services application is the registration software to manage access control for NHS Smartcards and facilitate the interface to ESR.

**Child Organisation** – an organisation that carries out some or all RA activities under a RA host organisation.

**Electronic Government Interoperability Framework (eGIF)** - defines the technical policies and specifications governing information flows across government and the public sector. They cover interconnectivity, data integration, e-services and content management.

**Electronic Staff Record** (**ESR)** - is the integrated Recruitment, HR, Payroll and learning management system in place within the Trust.

**ESR-CIS Interface** - ESR-CIS Interface can be used to link staff members’ records in ESR to user records in CIS in order to remove duplication and to drive access control based on the job that a person holds.

**Good Practice Guidance 45 (GPG45)** – provides UK government guidance on how to check someone's identity.

**Integrated Identity Management** (**IIM)** - is the combining of the parallel activities undertaken within Human Resources and the Registration Authority to create a single integrated process that reduces duplication.

**Local Smartcard Administrators** – Also sometimes referred to as PIN resetters, are staff members working in suitable roles across the Trust that have the ability to renew Smartcard certificates and unlock Smartcards (when the user has forgotten their passcode, or PIN) for other Smartcard users on their ward or in their department (other than those staff members that have been assigned the role of Sponsor, RA Manager, Advanced RA Agent or RA Agent).

**Position Based Access Control (PBAC)** - grants access to applications according to the position to which the staff members are assigned.

**Personal Demographics Service (PDS)** - are electronic records containing demographic information about patients and their NHS Number.

**Physical Smartcard** – An approved physical card supplied by the authorised supplier of cards to NHS Digital and, subsequently, the Trust, similar to chip and PIN bank cards.

**Registration Authority (RA)** – an official, or committee, within the organisation who is responsible for ensuring that all aspects of registration services and operations are performed in accordance with national Registration Authority policy and procedures.

**Registration Authority (RA) Agent** – Has the ability to grant requests approved by Sponsors and subsequently print Smartcards for new applicants as well as the ability to renew Smartcard certificates and unlock Smartcards for other Smartcard users (other than those staff members that have been assigned the role of Sponsor, RA Manager or Advanced RA Agent).

**Registration Authority (RA) Agent Identity Checker -** Has the ability to check user's identification and grant the digital identity. RA Agent ID Checkers do not have the ability to print Smartcards and grant access assignment requests in CIS.

**Registration Authority (RA) Manager** – Staff member within the RA who has overall responsibility for local Registration Authority processes and governance.

**Senior Information Risk Owner (SIRO)** - an executive who is familiar with and takes ownership of the organisations' information risk policy and acts as advocate for information risk.

**Summary Care Record** (**SCR)** - is an electronic record containing information about any medicines being taken, allergies or bad reactions to medicines previously taken.

**Smartcard** – Physical, virtual or other device, such as an iPad, which enables healthcare professionals to access clinical and personal information appropriate to their role on the Spine.

**Spine** – The Spine is a set of national services used by the National Care Records Service which includes PDS, SCR and SUS.

**Sponsors** – Sponsors are appointed and entrusted to act on behalf of the Trust Executive team in determining who should have access to applications, the level of access required and maintaining the appropriateness of that access.

**Staff members** – People who are directly employed by, or contracted to provide service to, or are part of an agreement with the organisation.

**Secondary Uses Service (SUS)** - uses information from patient records to provide anonymised business reports and statistics for research, planning and public health delivery.

**User's Unique Identification (UUID)** – the unique number identifying a user of Spine compliant applications. It is the long number that appears on a Smartcard.

**Virtual Smartcard** – A solution that provides the same access functionality as a physical Smartcard but the card itself may be stored on a device or in the cloud.

## 5. Duties and responsibilities

### Role of the Chief Executive

The Chief Executive has overall accountability for all aspects of policy setting and implementation.

### Role of the Trust Executive Team

The Executive Team are responsible for:

- ensuring that there is a Board or Executive Management Team level individual who is overtly identified and named and has overall accountability in the organisation for RA activity and for formally appointing the RA Managers and the Sponsors.
- ensuring that the necessary systems and resources are in place for the successful implementation and ongoing operation of this policy

***The Director of Digital has been identified as the accountable director for RA***

### Role of the Caldicott Guardian

The Trusts' Registration Authority reports to the Information Governance Steering Committee (IGSG) which is chaired by the SIRO and attended by the Caldicott Guardian.

The Caldicott Guardian has an advisory role regarding all matters of patient confidentiality and information sharing.

### Role of the Senior Information Risk Owner (SIRO)

The SIRO is responsible for:

- Ensuring the work of RA is appropriately monitored
- Ensuring all staff are aware of the importance of secure working practices in respect of Smartcards
- Ensuring there is effective governance in place so that the system access assigned to staff is appropriate to their role(s)
- Authorisation and approval of any new or amended Access Control Positions

**Role of the Information Governance Committee**
The Trust's Information Governance Committee/Sub Committee is responsible for:

- Approval and ratification of this Policy
- ensuring that it is disseminated to all relevant staff
- monitoring compliance with this policy

**Role of the Managers**
Managers who have responsibility for recruitment or who have been appointed as a Sponsor, are responsible for:

- reading this policy and ensuring that they understand its contents
- implementing and monitoring the operation of this policy within their functional, areas
- ensuring that staff always follow and adhere to this policy
- taking positive action to promote the security of electronic records ensuring that processes and procedures are in place to facilitate effective compliance with this policy, particularly during a major incident
- informing workforce when a member of their staff, that has been issued a smartcard, leaves the organisation or changes role
- reporting breaches of policy and, when required, taking the necessary supervisory or disciplinary action when infringements take place

**Role of ESR (Workforce) Administrators**
The ESR (Workforce) Administrator is responsible for receiving and processing the completed assignment form for staff members directly employed by ASPH after viewing the identification documents required.

Where these are in order, an addition to ESR will be made; the ESR Administrator should assign the user an ESR Position. Where the new staff member has an existing Smartcard the ESR Administrator will perform a search and link the Spine registration to ESR. Where a Smartcard needs to be issued, either new or replacement, this will be requested by the ESR Administrator through ESR RA Workbench. Any other actions or queries will be raised by the ESR Administrator through ESR RA Workbench.

The ESR Administrator is specifically responsible for:

- implementing the procedural documents at the local level
- updating ESR records for staff members directly employed by the organisation in accordance with the line manager's requirements which may include changing the ESR assigned position
- ensuring that the national RA processes are adhered to
- escalating any process, hardware, and application problems to the RA Manager
- ensuring that all forms and any other material which supports the issue/ revocation of a Smartcard and the position associated with the card are retained in accordance with the Trust Records Retention Policy
- ensuring that activities relating to the Registration Authority Agent and/or Registration Authority ID Checker function follow the Trust information governance policies and procedures.

**Role of the Registration Authority**
The Registration Authority (RA) is a virtual team within ASPH who are collectively responsible for ensuring that all aspects of registration services and operations are performed in accordance with national policies and procedures.

They are responsible for providing arrangements that will ensure tight control over the issue and maintenance of both physical and virtual Smartcards, whilst providing an efficient and responsive service that meets the needs of the users.

The Registration Authority is constituted from personnel within Digital Services, Workforce and medical education departments who have been designated the following RA roles:

- Registration Authority Manager
- Deputy Registration Authority Manager(s)
- Advanced Registration Authority Agents
- Registration Authority Agents
- Registration Authority ID Checker

The Registration Authority is responsible for:

- ensuring that all aspects of registration services and operations are performed in accordance with national policies and
- ensuring that any local processes developed to support the national registration processes are adhered to
- ensuring that any emergency processes developed to support the Trust during a major incident are adhered to and that robust processes exist to assist with the return to business as usual
- ensuring that there is sufficient availability of resource to operate the registration processes in a timely and efficient manner to meet their organisational responsibilities

- implementing the procedural documents at the local level
- issuing Smartcards to the relevant staff members who have proven identities
- updating CIS records for staff members in accordance with the line manager’s requirements which may include changing the assigned position
- revoking Smartcard access in accordance with the line manager’s requirements
- escalating any process, hardware, and application problems to the RA Manager
- ensuring that all copies of identity documents and other material which supports the issue/revocation of a Smartcard and the position associated with the card are retained in accordance with the Trust Records Retention Policy
- ensuring that activities relating to the Registration Authority Agent function follow the Trust information governance policies and procedures
- ensure that any positions and associated profiles are reviewed regularly, and accuracy is maintained

**Role of the RA Manager**

The RA Manager is responsible for providing a comprehensive RA service. This includes establishing an RA team, developing robust processes, auditing compliance with process and the production, review, and update of this policy.

The Trust authorises two deputy RA Managers to provide continuity in terms of day to day management whenever the lead RA Manager is not available.

The RA Manager is responsible for:

- appointing and managing a team of RA Agents to ensure that schedules and rotas are devised to accommodate the Trust’s RA requirements
- managing the day to day operation of the local Registration Authority
- ensuring that the national RA processes for Smartcard issue/revocation and profile modification are adhered to within the Trust, and any child organisations
- ensuring that the RA team members are adequately trained, including those of any child host organisations
- ensuring that the RA team members are familiar with any emergency processes developed to support the Trust during a major incident
- ensuring RA Agents are familiar with and understand the practice for identity checking, the setup and operation of the Registration Authority and this document
- escalating any process, hardware, and application problems to the notice of appropriate NHS national groups
- providing support to Advanced RA Agents, RA Agents, Sponsors and Local Smartcard Administrators on process, hardware, and application problems
- monitoring training compliance of the RA team members and ensuring that they are familiar with the local and national RA processes

- facilitating the process for agreeing the Trust access control positions
- verifying user's identity to GPG45 Level 3 or 4
- ensuring the Registration Authority functions in compliance with the Trust information governance policies and procedures
- undertaking regular audits of processes and procedures
- receiving and reporting on any incidents relating to RA policy and process
- responsible for maintaining and managing an audit trail of all Smartcards issued by the Registration Authority and access granted and revoked
- maintaining an inventory of all RA equipment including Smartcards and ensuring that all is in good working order
- professional accountability to uphold good RA practice to NHS Digital

**Role of the Registration Authority Agents**
The RA Agent is responsible for receiving Smartcard applications and, after viewing the identification documents required, access and additions to CIS will be made. The RA Agent takes or uploads a photograph and prints and issues the Smartcard. If position assignments have not been fulfilled through ESR, the RA Agent will assign the user the position which has been indicated by the Sponsor.

The RA agent is specifically responsible for:

- implementing the procedural documents at the local level
- verifying user's identity to GPG45 Level 3 or 4
- issuing Smartcards to the relevant users who have been sponsored and who have proven identities in accordance with the national process
- updating Smartcard profiles in accordance with the sponsor's requirements which includes adding and removing positions
- cancellation of Smartcards in accordance with the sponsor's requirements
- providing Smartcard maintenance services such as card unlocking, passcode renewal, certificate renewal and Smartcard replacement
- maintaining good working practices in respect of ESR/CIS interface to ensure that Smartcards are issued in a timely manner to appropriate personnel
- keeping Smartcards securely stored until issued
- maintaining a record of all Smartcards issued
- maintaining a record of all requests and active assignments for non-ASPH employed individuals
- ensuring that the national RA processes are adhered to within the Trust
- ensuring Smartcard users comply with the NHS Care Records Service Smartcard Terms and Conditions

- escalating any process, hardware and application problems to the RA Manager / Deputy RA Manager
- ensuring that activities relating to the Registration Authority Agent function are in compliance with the Trust information governance policies and procedures.
- supporting Smartcard holders signed up to the self-registration service
- attending training as required

**Role of the Registration Authority ID Checker**

The RA ID checker is responsible for:

- undertaking identity verification checks in line with this policy and national policy
- verifying user’s identity to GPG45 Level 3 or 4
- taking photographs when required
- attending training as required

**Role of the Registration Authority Sponsors**

The responsibilities a Sponsor has for their organisation are:

- approve user registrations as defined by the Executive Management Team and the Trust
- be familiar with the different types of Access Control Positions to approve
- work with RA agents to maintain access to Spine compliant applications within their area of responsibility that is consistent with the “NHS Confidentiality Code of Practice”
- be familiar with the applications they Sponsor users for via briefing material from the application providers
- complete any local training requirements
- specified Sponsors will be responsible for the assignment of Short Term Access cards and must maintain a register of who and when these are issued to

**Role of the Smartcard Unlocker / Local Smartcard Administrator**

A staff member assigned the role of a Smartcard Unlocker is responsible for:

- unlocking Smartcards for all staff, except for RA Agents and RA Managers
- attending training as required

**Role of the Privacy Officer**

The privacy officer is nominated by the Caldicott Guardian and reviews alerts generated automatically by privacy reports on Spine connected systems.

Alerts are generated in response to the following actions:

- A Smartcard user claims a legitimate relationship with a patient (self-claiming)

- A Smartcard user overrides a patient’s dissent to information sharing and accesses sensitive personal data about the patient that is being maintained by another legal organisation
- A Smartcard user accesses sensitive personal data about the patient that is maintained by another legal organisation, where the patient has permitted information can be shared
- A Smartcard user accesses information that has been ‘sealed’ at the patient’s request

The Privacy Officer is responsible for:

- Running or receiving privacy reports
- Audit and review of privacy reports and alerts
- Investigating any anomalies presented through privacy reports
- Reporting identified breaches

**Role of Staff Issued with a Smartcard**

The staff member is responsible for the correct daily usage of their Smartcard in line with their job role and associated business functions, ensuring that the card is never used by others and their passcodes are never comprised.

If the staff member believes their passcode to be compromised, they are responsible for changing it immediately. Advice can be sought via their Sponsor, the RA Manager, or a member of the RA Team.

All staff members issued with a Smartcard are responsible for:

- providing documentation to verify identity
- making themselves aware of the procedural documents relating to Smartcard usage
- complying with this policy
- complying with the NHS Care Records Service Smartcard Terms and Conditions
- raising any queries about the implementation of Trust Documents with their line manager or the RA Manager
- alerting their line manager of any non-compliance with this policy
- ensuring that they always have their Smartcard and passcode available when on duty
- keeping their Smartcard safe and secure and use it only in accordance with Trust policies and procedures
- reporting promptly to the RA Agent, RA Manager or Sponsor the loss or damage to their Smartcard to allow remedial action to get place
- maintaining compliance with Data Security Awareness/IG training

- being signed up to the self-registration service

# 6. Policy

### Smartcard Registration

***For employed staff***

ASPH operates an integrated process for HR and RA in that the identity verification element of the Registration Authority function for employed staff is encompassed within the Workforce department.

For the context of this policy the term “employed staff” is taken to be all individuals that are registered on ESR under ASPH.

Due to the sensitive data that can be accessed using a Smartcard, it **must** be the Line Manager that requests the Smartcard for their member of staff.

Requests are made to the Workforce team generic email asp-tr.esrinfo@nhs.net

The staff members information that needs to be provided in the email includes:

- Staff Members Full Name (this must be the full legal name as evidenced on identity documents)
- Date of birth
- National Insurance number
- If they have a smartcard from a previous Trust, their UUID number (located below their Smartcard photo)
- What system(s) they need access to
- What Access Control Position is required
- Staff email address
- Any workgroups that need to be assigned

Once this has been completed the Workforce team will record the identity checks in ESR. The ESR person record will be associated to CIS and a request made through ESR RA Workbench to produce the Smartcard.

The IT Training Team monitor the CIS Request Worklist for new requests. The IT Trainer checks requests are complete and valid, locates the relevant photograph and prints the Smartcard. Where a photograph is not available, the IT Trainer will contact the member of staff to arrange an appointment to take the photograph.

***For Non-ASPH Employed individuals***

For the context of this policy the term “non-ASPH employed” is taken to be all individuals that are **not** registered on ESR under ASPH; and can include students, locums and other temporary staff as well as individuals from partner organisations who require access to Smartcard systems as part of pathway of patient care.

A register of non-employed access requests and approvals will be maintained by the RA Agents.

A User Registration Application form must be completed, signed by an approved Sponsor and submitted to the IT Training Team generic mailbox asp-tr.it.training@nhs.net along with:

- evidence of completion of compliant Data Security Awareness/IG Training
- Date of birth
- National Insurance number
- If they have a smartcard from a previous Trust, their UUID number (located below their Smartcard photo)
- What system(s) they need access to
- What Access Control Position is required

All requests will require approval from the IG Manager and a member of the Digital Services senior management team.

Once approved the RA Agents will process the request as follows:

***New registration***
The individual will be invited to attend a Smartcard registration session in person with their identity documents. If identity is proven, registration on CIS will be undertaken and the Smartcard will be issued with the requested Access Control Position with an end date no greater than 12 months from approval.

***Existing Smartcard***
Where the individual has an existing Smartcard issued by another Trust, the RA Agent must establish a likeness between the holder and the Smartcard photograph before assigning positions. In the case of any doubt, the holder may be asked to present personal identification.

Once identity is established the requested Access Control Position will be assigned through CIS with an end date no greater than 12 months from approval.

**Registration and issuing of Smartcards during a Major Incident**
During any major incident that prevents the in person face-to-face requirements for the RA registration process identity checks may be carried out virtually using a combination of electronically provided copies of relevant identity documents and a provided passport-sized photograph, along with an identity check undertaken with the applicant using video conferencing software.

Smartcards **may** be issued unlocked, only in accordance with the national guidance procedure[2], by the RA Agent and posted to the most appropriate Local Smartcard Administrator, relevant Sponsor or the workplace address provided by the applicant.

For an unlocked Smartcard the passcode should be a randomly generated 6-digit passcode. The passcode must be conveyed to the staff member in a separate communication and only upon confirmation by the receiver of safe receipt and only having further verified their identity.

Where the receiver is unable to visit the workplace to collect the physical Smartcard, the RA Agent may post the Smartcard to the individual's home address in an unlocked state as above, remembering to include the Smartcard in a separate envelope marked "NHS Smartcard Enclosed" inside the addressed envelope. The outer envelope must be marked "Private Emergency Registration Authority (Smartcard) and Confidential, Addressee Only" with the RA Agent's return address clearly visible on the outer envelope.

### Smartcard Photographs

A Smartcard must bear the photograph of the user. Where a user is not known and is in possession of a Smartcard issued by another Trust, if there is any doubt about the accuracy of a Smartcard photograph it may be necessary for an RA Agent or RA Manager to see original personal identification.

### Handover of Smartcards

For new joiners, Smartcards will be handed over during induction or at relevant systems training. On receipt, the Smartcard user will be required to accept the online terms and conditions, register for self-service, and create their own PIN code.

All pre-printed Smartcards, or cards not issued immediately, are issued in a locked state. If not collected face-to-face the Smartcard user will need to present their Smartcard to a Local Smartcard Administrator / Smartcard Unlocker before it can be used.

### Change of Name

Individuals **must** provide documentary evidence e.g. marriage certificate, when requesting a change of legal name.

### Leavers

*Leavers moving to another NHS Organisation:*

If the destination of the leaving individual is another NHS organisation the individual should retain their Smartcard. Any positions relating to the employment with this Trust will be removed.

*Leavers not moving to another NHS Organisation:*

The Smartcard should be surrendered as part of the leavers process and returned to the RA team for destruction. Any positions relating to the employment or business function with this Trust will be removed.

[2] https://digital.nhs.uk/services/registration-authorities-and-smartcards/remote-smartcard-registration-emergency-guidance

**Unused Smartcards**

All Smartcards that are no longer required must be returned to the RA Team for cancellation and destruction.

**Lost or Stolen Smartcards**

Lost or stolen Smartcards need to be reported as an Incident in accordance with the Trust's Incident Reporting Policy.

A replacement Smartcard will need to be requested through the IT Training Team asp-tr.it.training@nhs.net

**Smartcard Certificate Renewals**

Smartcards have certificates that expire every 2 years. A warning will be presented when the certificate renewal is approaching.

Users should renew their own certificates by following the prompts on the self-service portal.

If a user fails to renew certificates within the stipulated period, the Smartcard will expire and only an RA Agent or RA Manager will be able to review and renew at a face-to-face meeting.

**Smartcard destruction and disposal**

All Smartcards requiring destruction must be returned to the RA Team c/o IT Training, Chertsey House, St Peter's Hospital.

The RA Team will destroy and dispose of all faulty, cancelled, unused Smartcards.

**Smartcard Incident Reporting**

All staff employed by or working on behalf of the Trust have a duty to report untoward incidents regarding Smartcard access or Smart card use.

Smartcard misuse refers to breach in the conditions of use/and or associated privileges including:

- Smartcard sharing
- Disclosure of Smartcard PIN
- Misuse of applications accessed with a Smartcard
- Smartcard theft or loss
- Repeated loss of Smartcard
- Non-compliance of local or national RA policy
- Unauthorised access of Spine compliant applications

The incident should be reported in accordance with the Trust Incident Management policy.

After investigation any further recommended action will be taken which may lead to disciplinary action.

The SIRO may refer to the Information Governance Steering Group to decide whether working practices should be reviewed as a result.

**Other related processes**
The processes supporting the identification, registration and management of users are integrated with other Trust processes as appropriate i.e., the recruitment process, starters and leavers process.

RA Policy and RA procedures are subject to audit by internal and external auditors. Audits would typically cover:

- the issue of Smartcards
- the management of Smartcards
- the profiles associated to uses in relation to their employed roles
- the use of Smartcards
- the use of systems requiring smartcards
- identity management
- security of supplies and equipment

**Security (Administration, Data Protection and Records)**
The Trust has designated the RAMs to be responsible for all administrative processes and ensuring compliance with NHS Digital policies and associated requirements.

All documentation and photographic information concerning registration identity must be kept in accordance with Trust policies.

All information relating to the verification of identity is to be treated as strictly confidential and used only for the intended purpose.

Any misuse of information by staff whose role includes RA elements will be dealt with under the Trust's disciplinary procedure.

Access to unused Smartcards will always be restricted; unused Smartcards will be kept in a secure location.

Smartcards must be removed from Smartcard readers when users are away from their device and/or desk to avoid possible Smartcard misuse, loss, or theft. This is particularly important where devices are shared.

**RA Reports**
CIS provides a set of standard reports that can be accessed by RA Managers and RA Agents.

Reports that contain user information such as name or UUID are:

- only accessible by RA staff, staff with RA responsibilities as described in this policy, or by those who are directly involved in enabling Smartcard access

- protected from non-RA users in keeping with policy and guidance on person identifiable data
- only circulated between RA Managers and RA Agents
- kept physically secure
- disposed of confidentially when no longer required

Reports will be used to actively manage the quality of registrations and access profiles associated with users in the organisation.

Reports should be periodically produced to monitor and improve the quality of RA information.

# 7. Training

Training on both the ESR and CIS systems is essential for the ESR Administrators, RA Agents and RA ID Checkers. This will maximise the knowledge of the two systems to ensure that they can use the systems as per the requirements specified by their employing organisation and NHS Digital.

Training to all RA Agents and RA ID Checkers will be provided by a Lead or Deputy RA Manager.

# 8. Stakeholder Engagement and Communication

This policy has been developed in accordance with the National RA Policy and guidelines, with the involvement of the Trust Digital Services department, the Trust Workforce team and the members of the Information Governance Steering Group.

# 9. Approval and Ratification

The policy will be approved and ratified by the Information Governance Steering Group.

# 10. Dissemination and Implementation

The policy will be disseminated through the Aspire global email and published on the organisation intranet and internet sites.

The Information Governance Steering Group is responsible for the implementation of this policy, including monitoring compliance.

# 11. Review and Revision Arrangements

This policy will be reviewed every 3 years in line with Trust policy; or updated in line with any new legislation issued or change in procedures; or when there is a change in national RA policy or guidance.

A revision will be triggered when there is a requirement to amend the name of individuals referenced below:

| RA Role | Full Name | Job Title |
|---|---|---|
| Accountable Director for RA | Laura Ellis-Philip | Director of Digital |
| Lead RA Manager | Nicola Rayment | Head of Digital Programme Delivery |
| Deputy RA Manager | Jonathan Spinks | Digital Programme Manager |
| Deputy RA Manager | Samantha Radford | IT Training Lead |
| Privacy Officer | Jane Townsend | Information Governance Manager |
| Senior Information Risk Owner | Laura Ellis-Philip | Director of Digital |
| Caldicott Guardian | David Fluck | Medical Director |

# 12. Document Control and Archiving

This is a Trust-wide document and archiving arrangements are managed by the Quality Department, which can be contacted to request master/archived copies.

# 13. Monitoring compliance with this Policy

| Measurable Policy Objective | Monitoring/ Audit method | Frequency of monitoring | Responsibility for performing the monitoring | Monitoring reported to which groups/ committees, inc responsibility for reviewing action plans |
|---|---|---|---|---|
| RA asset register compliance | Reports of RA hardware and consumables audits will be produced quarterly,<br>RA hardware and consumables audits will be made available as part of requisite evidence required to fulfil the requirements of | RA hardware and consumables will be audited at least quarterly | RA Manager(s) | Information Governance Steering Group |

| | | | | |
|---|---|---|---|---|
| | the NHS digital Statement of Compliance Data Security and Protection toolkit | | | |
| Controls for Non-ASPH employee assignments | A review of non-ASPH employee assignments with a sample audit for evidence supplied | Quarterly | RA Manager(s) | Information Governance Steering Group |
| Management of Access Control Positions | Review of all active and assigned positions | Annual | RA Manager(s) | Information Governance Steering Group |

## 14. Supporting References / Evidence Base

Good Practice Guide 43 – Requirements for Secure Delivery of Online Public Services
https://www.gov.uk/government/publications/requirements-for-secure-delivery-of-online-public-services

Good Practice Guide 44 – Authentication and Credentials for use with HMG Online Services
https://www.gov.uk/government/publications/authentication-credentials-for-online-government-services

Good Practice Guide 45 – Identifying Proofing and Verification of an Individual
https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual

National RA Policy
https://digital.nhs.uk/services/registration-authorities-and-smartcards#registration-authorities

NHS Confidentiality Code of Practice
https://www.gov.uk/government/publications/confidentiality-nhs-code-of-practice

Registration Authorities Operational Process and Guidance
https://digital.nhs.uk/services/registration-authorities-and-smartcards#registration-authorities

The Care Record Guarantee
https://digital.nhs.uk/binaries/content/assets/legacy/pdf/1/8/care_record_guarantee.pdf

Remote smartcard registration – emergency guidance for Registration Authorities
https://digital.nhs.uk/services/registration-authorities-and-smartcards/remote-smartcard-registration-emergency-guidance

# APPENDIX 1: EQUALITY IMPACT ASSESSMENT

### Equality Impact Assessment Summary

**Name and title:** Nicki Rayment – Head of Digital Programme Delivery (RA Manager)
**Policy:** Registration Authority (RA) Policy

| |
|---|
| **Background**<br>• Who was involved in the Equality Impact Assessment |
| The Trust's RA team constituting staff from Digital Services and Workforce teams; and members of the Information Governance Steering Group. |
| **Methodology**<br>• A brief account of how the likely effects of the policy was assessed (to include race and ethnic origin, disability, gender, culture, religion or belief, sexual orientation, age)<br>• The data sources and any other information used<br>• The consultation that was carried out (who, why and how?) |
| The policy was assessed as not impacting upon an individual's race and ethnic origin, disability, gender, culture, religion or belief, sexual orientation, age.<br>The information was a review of policy itself.<br>Consultation was therefore considered not applicable in this case. |
| **Key Findings**<br>• Describe the results of the assessment<br>• Identify if there is adverse or a potentially adverse impacts for any equalities groups |
| No adverse or potentially adverse impacts have been identified for any equalities groups; the policy affects all staff equally. |
| **Conclusion**<br>• Provide a summary of the overall conclusions |
| As outlined in methodology section. |

| |
|---|
| **Recommendations**<br>• State recommended changes to the proposed policy as a result of the impact assessment<br>• Where it has not been possible to amend the policy, provide the detail of any actions that have been identified<br>• Describe the plans for reviewing the assessment |
| No changes recommended. |