Policy:

HR O45 - Registration Authority (Smartcards)

Executive Director lead	Deputy Chief Executive
Policy Owner	Assistant Deputy Director of Informatics and Architecture
Policy Author	Digital Project Manager

Document type	Policy
Document version number	V2
Date of approval	28 April 2020
Approved by	Workforce & Organisation Development Committee (WODC)
Date of issue	10/05/2020
Date for review	31/03/2023

Summary of policy
This document is an updated Smartcard Policy for planned increased in implementation of Smartcards Trust wide in the near future.

Target audience	All staff who are issued Smartcards

Keywords	NHS Smartcard; Smart card; RA; Registration Authority; RA Manager; RA Agent. NHS Digital

Storage

Version 2 of this policy is stored and available through the SHSC intranet/internet. This version of the policy supersedes the previous version (V1.1 March 2015). Any copies of the previous policy held separately should be destroyed and replaced with this version.

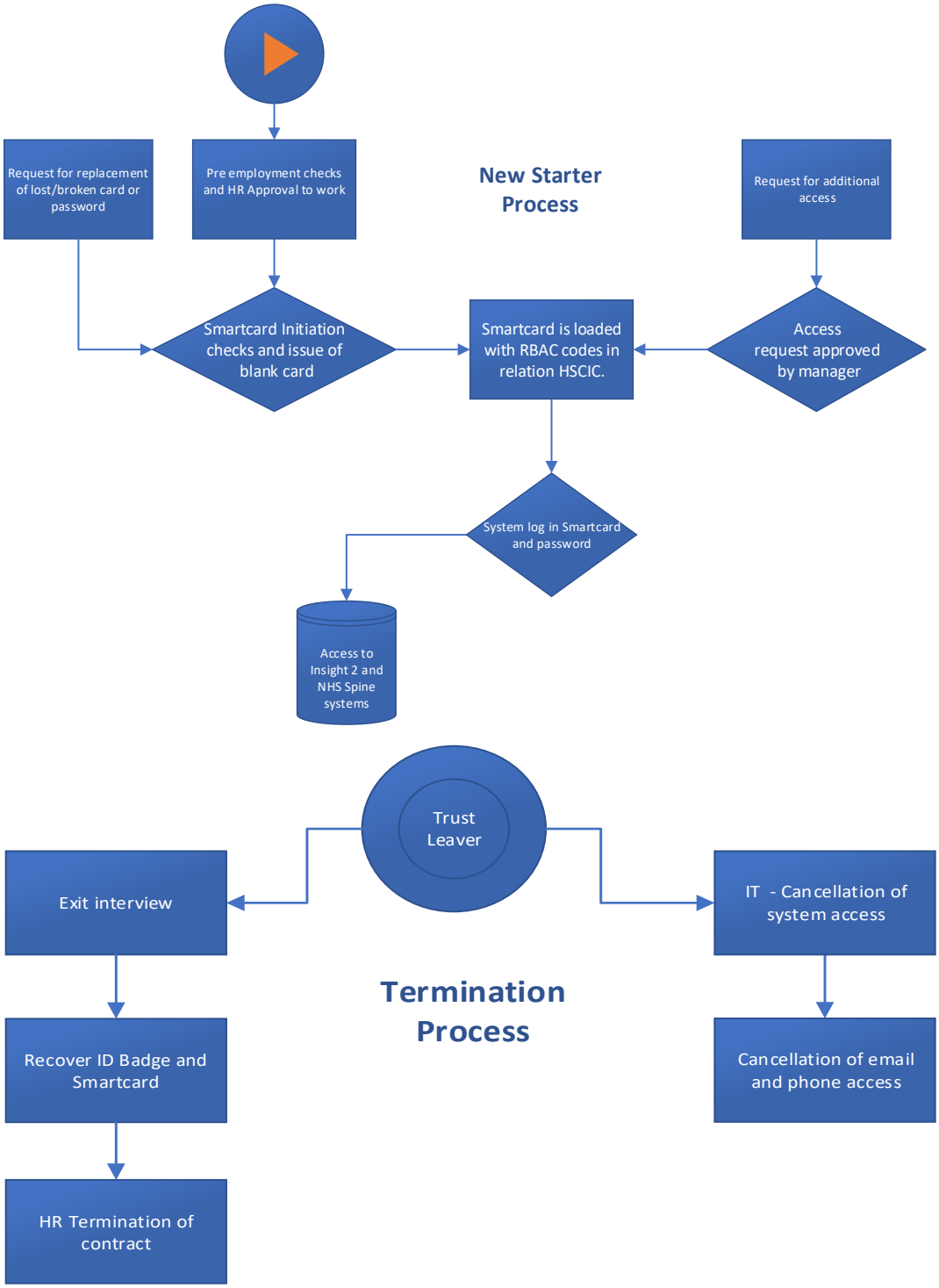
Version Control and Amendment Log

Version No.	Type of Change	Date	Description of change(s)
1.1	Revised policy created	2015	Revised Policy
2	Review, consultation, approval, ratification, issue	2020	• the policy reflects current national guidance and best practice as a CQC 'Must Do' requirement. • cross referencing to other policies has been undertaken and the appropriate section of the policy reflects this. • Workforce Information and other HR / IT colleagues reviewed the policy in April 2020. • Staff Side have considered the policy previously and indicated that they didn't have any comments on the policy. • The status of this policy will be minuted in the Joint Consultative Forum minutes 22nd April 2020. • Following consultation with HR / IT colleagues the following amendments have been made and the Amendment Log within the policy reflects this – - Updates to national guidelines - Agreement of the joint working between HR and IMST - The policy has been updated to allow for full Smartcard roll out across the Trust

Contents

Section		Page
	Version Control and Amendment Log	
	Flow Chart	1
1	Introduction	2
2	Scope	2
3	Purpose	2
4	Definitions	3
5	Details of the policy	4
6	Duties	5
7	Procedure	6
	7.1	6
	7.2 Training for RA Members	7
	7.3 Registration Authority Available Services	7
	7.4 Incident Reporting	7
	7.5 Responsibilities within the RA Function	8
	7.6 Registration Authority Manger	9
	7.7 Registration Authority Sponsors	10
	7.8 Registration Authority Agents	11
	7.9 The Smartcard User	12
	7.10 The Registration Authority Process	12
8	Development, consultation and approval	18
9	Audit, monitoring and review	19
10	Implementation plan	19
11	Dissemination, storage and archiving (control)	20
12	Training and other resource implications	20
13	Links to other policies, standards, references, legislation and national guidance	21
14	Contact details	21
	APPENDICES	
	Appendix A Equality Impact Assessment Process and Record for Written Policies	22
	Appendix B Registration Authority Identity Documents	23
	Appendix C What to do if no acceptable photographic personal identification documents are available	25

Flowchart


Request for replacement of lost/broken card or password
Pre employment checks and HR Approval to work
New Starter Process
Request for additional access
Smartcard Initiation checks and issue of blank card
Smartcard is loaded with RBAC codes in relation HSCIC.
Access request approved by manager
System log in Smartcard and password
Access to Insight 2 and NHS Spine systems
Trust Leaver
Exit interview
IT - Cancellation of system access
Termination Process
Recover ID Badge and Smartcard
Cancellation of email and phone access
HR Termination of contract

1. Introduction

To enable healthcare professionals to gain access to IT applications provided by NHS Digital they need to be issued with a Smartcard and to be registered with the Trust's Registration Authority (RA). NHS Digital produced a new Registration Authority Policy version 1.0 on 2 September 2014 to ensure all Registration Authorities align with the new Care Identity Services (CIS) application released in February 2015. The CIS application replaced the User Identity Manager (UIM) application. This policy has been updated to reflect the change in national requirements.

The primary purpose of NHS Smartcards is to provide identification and system authentication to local informatics applications. NHS Smartcards are a plastic card or a virtual Smartcard containing an electronic chip (like a chip and PIN credit card) that is used to access HSCIC applications, along with a Passcode. The chip stores the Unique User Identifier (UUID), providing a secure link between the HSCIC application and the NHS Spine) which holds the Users information and access rights. The combination of the NHS Smartcard and the Passcode together, help protect the security and confidentiality of electronically stored personal and sensitive data in line with the Care Record Guarantee. They allow access to applications via the NHS Care Records Service (CRS) and the Electronic Staff Record (ESR) but also define the level of access once within any individual application. The use of a smart card is mandatory for all NHS CRS compliant applications and Trust policies related to data and patient confidentiality are applicable, where relevant.

The registration process is operated at a local level by an authorised Registration Authority (RA) who are required to conform to the national Registration Policy and Practices. The operation of the Registration Authority is an integrated works between the Human Resources Department and IMST. In its current set up, the RA processes are for the vast majority is separate from other HR processes (for example many ID checks are done twice for one employee). For a streamlined process, creating profiles and doing ID checks would be sitting with HR, along with providing starters and leavers detailed information to the RA team, and the RA team would allocate access to systems, and close profiles for leavers/do any audit work as required.

The Registration Authority Policy is a vital aspect of information governance for the Trust since its primary responsibility is to maintain confidentiality of service user and employee personal data.

The policy also affirms roles/functions of the Registration Authority process.

2. Scope

This policy relates to the Registration Authority systems and processes and is applicable to employees, volunteers and students within the Trust. For those staff who are contracted to provide a service to or part of an agreement with the Trust this policy is also applicable whilst undertaking duties on behalf of the Trust or working on Trust premises and forms part of their agreement with the Trust.

3. Purpose

The Trust requires a Registration Authority to manage the distribution and use Smartcards. The registration process for the National Programme must meet the current Government requirements. The Registration Process is operated at a local level by a Registration Authority who are required to conform to the National Registration Policy and Practices identified below.

This policy describes procedures for the operation of the Registration Authority (RA) within Sheffield Health and Social Care NHS Foundation Trust (hereafter known as the Trust). The policy will outline the agreed processes required to support the ESR interface to CIS ongoing. Providing guidance to ensure that relevant applications continue to operate safely and efficiently through future developments.

All data and personal information about NHS Smartcard Users must be used in accordance with the GDPR Data Protection act 2018 principles. The Trust will comply fully with the latest published National Policies and Procedures identified in the following documents:

- Registration Authorities Setup and Operation (available from http://nww.npfit.nhs.uk/implementation/)
- Registration Authority Operating Guidance 2013/14 (available from http://systems.hscic.gov.uk/systemsandservices/rasmartcards/)
- RA Governance Framework “Registration Authorities: Governance Arrangements for NHS Organisations”.
- Registration Policy and Practices for Level 3 Authentications (available from http://nww.npfit.nhs.uk/implementation/)
- The NHS Confidentiality Code of Practice (www.dh.gov.uk)
- NCRS Acceptable Use Policy, Terms and Conditions (available from http://nww.npfit.nhs.uk/implementation/)
- The Care Record Guarantee

The purpose of the Trusts Registration Authority is to ensure that employees/individuals providing healthcare services to the NHS directly or indirectly have timely access to NHS CRS compliant applications (and information) in accordance with their role.

The Registration Authority (RA) is made up of Registration Authority Managers, Registration Authority Agents and Sponsors.

The Trust needs to ensure that all relevant users have timely access to patient and employee Information Technology systems to facilitate excellent care provision and contemporaneous record keeping within the Trust which the Registration Authority supports.

4. Definitions

CRS	Care Records Service
EDG	Executive Director Group
e-GIF	electronic Government Interoperability Framework
e-RS	Electronic Referral Service.
GDPR	General Data Protection Regulation) is a legal framework that sets guidelines for the collection and processing of personal information from individuals who live in the European Union (EU).
HR	Human Resources
HSCIC	Health Social Care Information Centre Its primary function is to collate the medical records of the patient population into a central database.
IMST	Information Management System and Technology
NHS-Digital	National body that SHSC is accountable to for Registration Authority services (formerly known as Health & Social Care Information Centre, HSCIC).
NHS-Smartcard	(often abbreviated to Smartcard) very similar to a chip and pin bank card.
RA	Registration Authority.
RBAC	Role Based Access Codes are a nationally defined set of codes that are used in conjunction with HSCIC access gateway to give staff access to specific systems. SHSC users are assigned specific codes to access the specific Trust data systems.
RA Owner	The person with the overall responsibility and oversight of the RA Process on behalf of the Trust. This is usually the Caldicott Guardian
RA Manager	Manages the RA Process on behalf of the RA Owner and manages the RA Agents.
RA Agent	Verifies the identity of staff, registers new users and removes system access for leavers.
RA Sponsor	Are usually, but not exclusively, managers who entrusted by SHSC to grant access clearance for a member of staff requesting access a restricted system and deciding on the appropriate level of that access appropriate to the role.
SHSC	Where used this relates to Sheffield Health and Social Care NHS Foundation Trust.
The Trust	Where used this relates to Sheffield Health and Social Care NHS Foundation Trust.
WI	Workforce Information, a function within HR that supports RA

5. Details of Policy

Details of this policy can be found in the introduction

6. Duties

Overall accountability for Registration Authority processes lies with the Director of HR, who has overall responsibility for establishing and maintaining effective and safe systems to manage and support access to electronic record systems through the use of Smart Cards

The responsibility for the processes within the Trust is delegated to the following individuals:

The Director of Human Resources has accountability for developing the Policy and maintaining an overview of the process. Should the RA Manager change it is the responsibility of the Director of Workforce and OD on behalf of the Chief Executive/ Senior Leadership Team, to notify the responsible person at NHS Digital of this change. The Director of Workforce and OD is also the Information Asset Owner (IAO) in relation to all aspects of the Registration Authority. The Director of Workforce and OD, on behalf of the Executive Management Team is responsible for confirming in writing to the RA function, the appointment of any RA Managers or agents.

The Director of IMST as the Senior Information Risk Owner (SIRO) is also responsible for and accountable to the Board of Directors for any information risks identified in relation to this and other Information Governance policies and procedures. The Director of IMST also has delegated responsibility for managing the development and implementation of Information Management and Governance policies and chairs the Information Governance Steering Group.

The Deputy Chief Executive/Director of Nursing has delegated responsibility for managing any clinical issues associated with the use of smart cards.

The Medical Director as the Caldicott Guardian acts as the conscience of the organisation in relation to the use and protection of all health and social care records.

The Registration Authority Manager is the designated lead for the Registration Authority process. The RA function for the Trust sits in the Directorate of Human Resources and the RA Manager is a Human Resources Manager. The RA Manager is accountable to the Director of Human Resources.

Registration Authority Sponsors RA Sponsors are appointed and entrusted to act on behalf of the Trust in determining who should have what access and maintaining the appropriateness of that access. Sponsors are appointed on behalf of the Executive Management Team by the Director of Workforce and Organisational Development. The nominated sponsor will then arrange a meeting with the RA Team, either with an RA Agent or RA Manager, for their Sponsor rights to be processed, presenting the letter from the Director of Workforce and Organisational Development and their proof of identify documents.

Registration Authority Agents RA Agents are responsible to the RA Manager for ensuring that the national and local processes are followed and for the accurate input of information on RA forms onto the NHS Spine NCRS Smartcard Management Service. RA Agents are part of the Human Resources Department.

Registration Authority Team For the purpose of this policy the term 'Registration Authority Team' means the Registration Authority Agents and Registration Authority Managers who work collaboratively to ensure the delivery of an efficient and effective registration authority function.

Local Smartcard Administrators A Local Smartcard Administrators (LSA) is an individual selected and trained by the Trust's RA Manager or RA Agent to help support the RA function with the unlocking of Smartcards and the renewing of expiring certificates for other Smartcard users within their directorate.

Applicant (Healthcare professionals) The applicant for a smartcard is responsible for the safe use and storage of their smartcard. The card should be treated with care and protected to prevent loss or damage. The applicant should ensure that no other person uses or has access to their card, account, or passcode. The key roles and responsibilities and the information flows within a Registration Authority are demonstrated as follows;

IT Manager and IT Help Desk - The IT Manager is responsible for ensuring that there is sufficient computer equipment to support all users of CRS applications (including those for registration). Any failure or unavailability in NHS CRS compliant applications are reported to the IT Helpdesk in the first instance. The IT Helpdesk are responsible for logging the incident with the National Service Desk, where applicable.

7. Procedure/Implementation

7.1 The local Registration Authority ensures that individuals providing healthcare services to the NHS directly, or indirectly, have access to NHS CRS compliant applications/information in accordance with their role. It is the Trusts responsibility to ensure that the requirements of RA's are met and maintained to adhere to the *"NHS Confidentiality Code of Practice"* and the *"Care Record Guarantee"*.

The RA responsibilities are defined as follows;

- Ensuring that the RA requests via CIS Worklist or RA Forms are appropriately completed and actioned
- Ensuring that any local processes developed to support the National Registration processes are adhered to in full
- Ensuring that there is sufficient availability of resource to operate the registration processes in a timely and efficient manner to meet the Trust responsibilities
- Ensuring that RA team members are adequately trained and familiar with the local and national RA processes
- Ensuring that an indexed and secure audit trail is maintained of applicant's registration information and profile changes via the CIS system. All completed application forms and associated documents are kept secure in an area where the RA team and wider HR team have access, in line with HSC 1999/053 which stipulates the retention duration for HR type records.

- Ensuring that there are sufficient Smartcards and Smartcard issuing and maintenance equipment for the organisation.
- Ensure sponsors identified via the Trust have the business function of “sponsor” associated with the appropriate organisation job profile/s.
- Monitoring compliance with the terms and conditions of smartcard usage.

7.2 Training for RA Members

All Trust RA Members will have sufficient training to carry out their RA tasks in accordance with National Policies and Procedures. They will be employees capable of trust as they will be handling sensitive information covered by The Data Protection Act.

7.3 Registration Authority Available Services

The services available will be:

- User Registration
- Position Based Access Control (PBAC)
  - adding Role/Position Profiles
  - changing Role/Position Profiles
  - deactivating Role/Position Profiles
- Revocation and cancelling of Smartcards
- User Suspension
- PIN/Pass-code resetting
- Smartcard renewal and exchange

7.4 Incident Reporting

Incidents may be reported by any member of staff where they feel that there is a risk to patient health, confidentiality or Trust reputation. Incidents should be reported, using the Trust Incident Reporting Policy, which will then be shared with the RA Manager. An employee must report suspected Smartcard misuse in line with Trust incident reporting policy and procedure via an Incident Reporting Form. Depending on the severity of the allegation an investigation may be required in accordance with the Policy and Procedure on the Management of Disciplinary Matters. If it is suspected that a Smartcard is being misused, then it should be reported to HR who may request that the certificate associated with the Smartcard should be suspended or revoked as appropriate.

Examples of incidents are:

- Smartcard or application misuse.
- Smartcard theft.
- Non-compliance of local or national RA policy.
- Any unauthorised access of CRS applications.
- Any unauthorised alteration of patient data.
- Unauthorised and inappropriate access to patient information.

The RA Manager will consider all incidents reported to them. Any incidents considered significant will be escalated within the Care Group and/or to the Caldicott Guardian depending on the nature of the incident. A major breach of

security will also be reported by the RA Manager to NHS Digital (if appropriate) to ensure any risks resulting from the event can be taken into account and mitigated against.

A significant incident is an isolated incident or a series of less significant incidents that could lead to a serious degradation of healthcare or information security. The Trust and the Caldicott Guardian will consider incidents reported to them and decide whether Trust systems or working practices should be reviewed as a result.

Any incidents involving breaches of security or demonstrate that a smartcard user may not be considered trustworthy may result in a disciplinary sanction, including dismissal in accordance with the Trusts Policy and Procedure for the Management of Disciplinary Matters.

The reporting of NHS CRS compliant applications failure or unavailability should be directed to the IT Helpdesk in the first instance. The IT Helpdesk will be responsible for logging the incident with the National Service Desk, where applicable. In such instances, operational services, departments and/or teams must revert to manual contingencies procedures.

7.5 Responsibilities Within the RA Function

Responsibilities of all Registration Authority personnel (excluding sponsors)

Identify areas where the Trusts business processes need integrating to minimise risk and duplication of effort.

- Complete the e-Learning modules available via NHS Digital or the Oracle Learning Management (OLM) system in Electronic Staff Record (ESR).
- Complete the required Information Governance training.
- Complete any local training requirements.
- Report all RA related security incidents as detailed in Section 5.4
- Ensure there is a sufficient supply of NHS Smartcards and RA hardware, including access to the Care Identity Service (CIS) for Sponsors (Smartcard unlocking and certificate renewal), and communicate technical requirements IMST through the Service Desk.
- Join the RA Community Site on NHS Networks to share knowledge and gain useful information as recommended by the NHS Connecting for Health http://www.networks.nhs.uk/nhs-networks/registration-authority-community.
- Produce NHS Smartcards, renew NHS Smartcard certificates and unlock NHS Smartcards for anyone at the same level or lower within the RA hierarchy.
- Be familiar with and adhere to this Policy and Registration Authorities: Governance Arrangements for NHS Organisations - https://bit.ly/2zbjdKj
- Ensure Users have only one NHS Smartcard issued to them showing their UUID and photograph, and that Users are aware of their responsibilities relating to Information Governance and NHS Smartcard Terms and Conditions
- Ensure Users are aware of the self-service functionality available to them, including how to unlock Smartcards, reset Passcodes, and renew Smartcard certificates
- Ensure the ESR and RA interface is maintained through the ESR position linking.

- Ensure an awareness of the appropriate identification documentation guidelines at NHS Employers as per National Policy

7.6 Registration Authority Manager

The primary responsibilities of the Registration Authority Manager are defined below:

- Assign, sponsor, and register RA agents (where permitted under governance arrangements), ensuring there are sufficient resources to operate the registration processes in a timely and efficient manner.
- Ensure the RA Team members are adequately trained according to the HSCIC guidelines.
- Implement an Audit policy and inventory of all RA kits.
- Identify a secure locked area for the storage of all paper-based registration documentation and associated information in accordance with the Data Protection Act 1998. This includes RA manager, RA agent, and Sponsor assignment documents, RA forms, RA reports, and inter-organisational agreements. All RA forms must be clearly marked with the User's UUID number and filed in a designated area
- Ensure all service issues are resolved through normal service, supplier or programme channels before escalating to the next level in the RA cascade.
- Disseminate National RA information to interested parties. For example, communicate PBAC information to Sponsors.
- Ensure there is a process for the renewal of NHS Smartcard certificates.
- Ensure adherence to national policies, procedures and guidance and when implementing locally, establishing RA governance frameworks i.e. Registration policy and practices for level 3 authentication, registration authority operational process and guidance.
- Ensure users have only one NHS CRS smartcard issued to them showing their User's Unique Identifier (UUID) and photograph, and that users are aware of their security and confidentiality responsibilities relating to smartcard use. The issue of more than one NHS CRS smartcard to a user is not permitted.
- Ensure compliance with procedures for lost, stolen, forgotten and damaged smartcards requiring urgent replacement.
- Inform the HSCIC of any process, hardware and application problems associated with the Registration Authority function through the National Service Desk (NSD).
- Where an organisation is merging or closing, identifying where the Registration Authority records will reside and gain approval from the Information Governance Steering Group.
- Liaise with local IT Services in ensuring compliance with up to date versions of Registration Authority related software across all of the local IT estate, as necessary.
- Represent the Trust at Registration Authority Leads forums both nationally and regionally as required.

7.7 Registration Authority Agents

The RA Agents will be responsible for the issuing and registering of the smartcard and inputting access levels in accordance with requests from the sponsors. They will also be responsible for reporting all incidents, misuses, anomalies and problems to the RA Manager and where relevant the Caldicott Guardian. The RA Agents are responsible for cleaning their printers on a monthly basis using the equipment supplied by the RA Manager, thus optimising the performance of the printer.

RA Agents can be registered and issued with Agent smart cards provided their role as RA Agent has been authorised/sponsored by the RA Manager.

RA Agents will

- Adhere to the Audit policy and ensure that all RA forms and associated information is maintained and securely stored according to national policy.
- Ensure that all activities relating to the Registration Authority Agent function are in compliance with the Trust's information governance policies and procedures.
- Renew a User's Smartcard certificates if confident of the User's identity, their identify will be confirmed by

  - The photograph on their Smartcard or via their Account Recovery Passcode,
  - If the identity cannot be verified, the applicant is required to produce documentary evidence to the RA.as detailed in Appendix One.
  - If the identity still cannot be verified, the incident is reported to the RA manager. It may be necessary to cancel or revoke the locked NHS Smartcard.

- Unlock a User's Smartcard and reset logon Passcodes."
- Ensure their contact details including email address and telephone numbers are recorded in the Spine User Directory.
- Perform CIS requests
- Ensure Smartcard users comply with the Terms & conditions by issuing the RA Information and running reports to confirm all staff have signed the electronic Terms & Conditions.
- The RA Agent will publish and maintain the list of sponsors and PBAC's available on the staff Intranet.

7.8 Registration Authority Sponsors

Sponsors will be identified by the Trust, or the Caldicott Guardian as being suitable persons by virtue of their status and role. Sponsors will be registered by an RA Manager or RA Agent on behalf of the Trust in accordance with instructions given by the Trust. Sponsors will be staff with sufficient seniority to understand and accept the responsibility required. Registration Sponsors are responsible to the RA Manager for the accuracy of the information on the RA Forms or CIS Requests.

Sponsors are responsible for approving access on behalf of the Trust, who can access what healthcare information, ensuring that users are given the minimum appropriate level of access needed to perform their job. Sponsors will be held accountable by the Trust for their actions. Sponsors are responsible to the Trust to ensure only appropriate access to CRS Applications is granted.

Sponsors will:

- Be familiar with the different types of Position Based Access Control (PBAC) to approve.
- Ensure that access profiles submitted to a Registration Authority follow PBAC material published by suppliers, on the RA website, or developed locally, and the implications of approving the access profiles.
- Work with RA agents to maintain access to NHS CRS compliant applications within their area of responsibility that is consistent with the “NHS Confidentiality Code of Practice”. This includes Access Control Position assignment and removal, and the revocation of NHS Smartcards and NHS Smartcard certificates.
- Be familiar with the applications they sponsor Users for via briefing material from the application providers.
- Complete the Sponsor e-Learning modules available via the HSCIC Premier IT Task website or the OLM system in ESR
- Complete the required IG training
- Complete any local training requirements

Sponsors will also be able to unlock smartcards and allow users to reset their PIN pass codes.

The RA Manager will keep sample Sponsor’s signatures for comparison with Sponsor’s signatures on RA forms. RA forms may be scanned and transmitted by fax or e-mail and sent to RA Agents for processing. The original RA form must be sent to the RA within five working days. Where this does not happen the RA agent will revoke the access rights which were allocated to the employee. Where forms have been emailed to the RA Team, the RA Team will periodically use the Account Recovery challenge to verify the Sponsor. In all cases where there is doubt over the signature compared to the RA sample signature the Account recovery challenge will be used.

Sponsors will work with RA Agents to maintain access to NHS CRS compliant applications within their area of responsibility that is consistent with the Informatics Security Policy. This includes access profiles/position change and removal, and the revocation of smartcards and smartcard certificates.

Sponsors will also

- Initiate requests to Registration Authority personnel through the RA form process for staff registrations and position/role assignments.
- Renew a user’s smartcard certificate (where applicable) and reset passcodes, – only where confident of the user’s identity.
- Unlock a user’s smartcard - only where confident of the user’s identity and that the appropriate Information Governance and IT Systems (e.g. Systm One) training has been completed. The smartcard user’s identify will be confirmed by the photograph on their Smartcard or via their Account Recovery Passcode, Should it be found that a card has been unlocked without appropriate training, this will be escalated to the relevant manager and may result in disciplinary action.
- Ensure that the position/role profile associated with a user is appropriate.

- Inform the RA Manager of problems associated with user access levels.
- Ensure that the Trust Incident Report Process is fully complied with for all instances where smartcards have either been lost, misplaced or stolen.
- Regularly review, at least annually, to confirm that all staff remaining in employment with the organisation are performing the same duties and have appropriate access levels assigned for their job role(s) and make requests to amend access rights in a timely manner, as appropriate. This information will be shared in summary format with the Human Resources and Organisational Development Policy and Planning Group.

7.9 The Smartcard User

The User is responsible for ensuring that if the card is lost or stolen this is reported as soon as possible to their Line Manager or to a member of the Registration Authority Team. The sponsor should then raise a request for a new card via CIS which the user can then arrange to collect in person from the RA team. The applicant must also complete an Incident Reporting Form/Safeguard Form.

The user is responsible for ensuring that they only use the smartcard to access the levels within an IT application for which they have a legitimate reason. The Trust monitors compliance with the Policy and terms and conditions of smartcard usage and unauthorised access will be considered as a breach of conduct and may result in disciplinary proceedings, including disciplinary action and dismissal. The applicant is responsible for keeping their PIN codes or pass codes confidential and must not share these or leave their card unattended at any time.

Incidents should be reported by any member of staff where they feel that there is a risk to patient, health, confidentiality or Trust reputation.

All users are responsible for their own compliance with information governance principles and for the safe and authorised use of smartcards. All employees are expected to familiarise themselves with the relevant information governance policies and undertake regular mandatory and statutory training updates. Staff not issued with smart cards should never use those issued to other people and have a duty to report any misuse which they become aware of.

7.10 The Registration Authority Process

Position Based Access Control (PBAC)

The patient information a User is able to access depends upon the position assigned to them via CIS on the Spine. CIS simplifies the registration process and strengthens the governance in two keyways:

- Use Position Based Access Controls to ensure consistency in granting access rights to individuals that have been formally approved by the organisation.
- All steps MUST have role separation - different individuals are required to approve and grant access rights. i.e. Staff assigned with Authorised Sponsor position can ‘Approve’ users at start of new registration process and an RA Agent/Manager can ‘Grant’ to complete the process after identity check requirements have been satisfied. (The terminology gets tricky here as there is the “role” for sponsor, agent, manager etc.)

Starters

As part of normal induction processes new staff required to use CRS will be:

- Introduced to the relevant Sponsor who will identify the appropriate PBAC for the user and take them through the Trust RA processes required.
- Trained on the aspects of CRS Application use relevant to their role/s.
- Trained on the National and Trust RA processes.
- Where full registration is required; the Applicant will be required to bring suitable forms of identification with them as detailed in Appendix One – Registration Authority Identity Documents.

Where staff are recruited to a role which requires access to National CRS Applications it is important that the following points are considered:

- Checks on an applicant's ID are made during smartcard application to ensure that e-gif Level 3 identification requirements can be met
- Offers of employment are dependent on the applicant's ability to meet and continue to meet all requirements for CRS access
- Induction processes include the issuing of Smartcards (where the applicant is not an existing Smartcard holder) and adding of the appropriate PBAC
- Employees should be trained sufficiently prior to the use of Smartcards and/or CRS Applications to ensure they carry out their CRS Application tasks without risk.
- Employees must digitally sign to acknowledge that they have read and understood the policies and procedures governing the use of Smartcards and CRS Applications. Users will be required to enter their passcode in CIS upon first registration to confirm they have read and agree to the terms and conditions. In instances where the RA team issue a card locked, a temporary passcode will be issued to enable users to agree, and the card will then be reset to a locked state and given to the user.
- All smartcards will be issued 'locked' unless the employee has completed their Information Governance Training. In addition, where the smartcard has been issued to allow the employee to access They must also complete the Systm One training prior to the smartcard being unlocked.

Leavers and Revocation

When staff are leaving, the following points must be considered:

- If the employee is transferring to another NHS related location e.g. GP practice, Acute Trust etc, then they may retain the Smartcard but their Trust profile must be removed.
- Employees leaving the NHS will have their certificate(s) revoked and the PBAC assigned to them in CIS removed. The user will retain the smartcard. Staff who use the ESR interface with CIS will automatically have the certificates revoked and PBAC removed once the person is terminated in ESR.
- The required actions must be taken as soon after the staff member leaves. Within the system it is possible to action the changes for a future date, therefore sponsors must action the RA documentation at the same time as completing the leaver form

- As a precaution the RA Agents will produce from the Electronic Staff Record (ESR) System a report detailing all leavers for the previous month, review this against the UIM requests which they have received and where anomalies are identified they will remove all access rights. The RA Agent will also be responsible for completing an Incident Reporting Form to detail the risk and addressing this with the relevant manager. The RA Agent will also share this information with the Systm One to ensure that their access rights are also closed down on the Systm One.

There are occasions when it is necessary to deactivate a Smartcard by revoking the Smartcard certificate. Reasons for this include:

- The Smartcard is lost or stolen
- There has been some other security breach associated with the Smartcard or Smartcard certificate.
- The user is no longer employed by an NHS organisation

Revocation tasks can only be carried out by RA Team Members and renders the Smartcard useless.

Where the revocation has been requested by HR because of security related events the RA Manager will authorise the appropriate action and inform the following staff as appropriate:

- The HR Representative
- The relevant Sponsor(s)
- The RA User

Should there be two incidents per annum where the same Sponsor has not actioned the paperwork for a leaver this will be escalated to the Sponsors manager for further discussion/action.

Changes to existing user access levels

What an employee/user is able to access is based on the information in the profile. Whenever there is a temporary or permanent change in the way an employee works, a review of their NHS CRS compliant application access must be carried out by a Sponsor. If there are significant changes to the staff member's role the relevant Role/ Position Profile on the NHS CRS compliant Spine User Database must be requested via a RA Sponsor. Some examples are listed below: -

- Changes to Job Title
- Changes to Access requirements
- Changes to Department
- Changes to Site(s) or base location

N.B. The ESR position has the CIS position(s) allocated to it.
The most common issue we have currently is where an ESR position is changed for a staff member independently from any reasons related to RA (which is the most common) but the RA position may accidentally be removed where the person still needs the access.

Where new roles/positions are being added or roles/positions are being changed the RA Sponsor of the relevant work area will discuss this in the first instance, and if supported the will be required to request changes via CIS, ensuring the end dates are stated where the role/position assignment is for a temporary period. Upon receiving the requests, the RA Agent will action the changes as detailed by the sponsor. Should there be any problems with the changes these will be referred to the signing Sponsor, prior to processing.

As a precaution the RA Agents will produce from the Electronic Staff Record (ESR) System a report detailing all changes for the previous month, highlighting where an employee has changed roles and/or teams, review this against the requests which they have received and where anomalies are identified escalate the anomalies to the appropriate Sponsor.

Locums, Agency and Bank Personnel

Temporary staff filling roles may need access to NHS CRS applications records as part of their role. The following points should be considered:

- Staff working as part of a team may not need a Smartcard to fulfil the role. A smartcard should only be issued to temporary/bank staff members if access to one or more NHS CRS applications is a key requirement of the role/s they will be fulfilling.
- Locums, agency and bank may not appear on the ESR reports. It will depend on how those staff's information is managed, currently, they are not consistently entered on ESR, and some agency staff are created profiles directly on CIS without going through the ESR/CIS interface.
- Some temporary staff could already hold a smartcard and will only require a role profile added
- Temporary staff who are Smartcard holders may not have sufficient training in the use of the particular CRS Application needed to be accessed.
- Should admin bank staff change teams then it is the responsibility of the Bank Admin Management function to complete the necessary RA forms to remove the access rights, as soon as it is known that the employee is leaving the team.

Management and use of RA Equipment

The RA Manager, on behalf of the Trust, will be responsible for ensuring that adequate numbers of Smartcards and Smartcard readers are available and maintaining the smartcards throughout their useful life. USB Smartcard readers can also be used. The IT Manager will ensure that there is sufficient computer equipment to support all users of CRS applications (including those for registration). All RA equipment will be subject to policies and procedures governing the management and control of Trust Assets.

Electronic Registration Authority Processes

The electronic system allows the sponsor to make requests in CIS.
Sponsors register a request in CIS for the following;

- Register a new user
- Assign a position

- Remove a position
- Close a user

The RA team will provide appropriate sponsor training as required. Sponsors can also contact the RA team directly for assistance.

As part of the move towards Integrated Identity Management and utilising the functionality of the CIS/ ESR Interface, the RA team will continue to work towards linking ESR positions with CIS positions.

Identity Requirements

Checks on an applicant's identity are carried out during the smartcard application process to ensure that e-gif level 3 requirements can be met. These requirements are in line with the most recent issue of the NHS Employers employment check standards on identity. A list of acceptable identification documents can be found in Appendix 1. Where an applicant is unable to provide the documentation specified in Appendix 1, alternative combinations may be accepted in line with the NHS Employers employment check standards.

Online documentation

Refer to NHS employer's guidance for what constitutes acceptable documentation.

Lost, Stolen and Broken Smartcards

Lost and damaged Smartcards should be reported to the RA Team as soon as is practicable by contacting emailing workforce@shsc.nhs.uk For any cards which are lost or stolen then an E-Incident Login must also be completed by the employee.

Once notified that a Smartcard has been lost or damaged an RA Agents will arrange to have the lost/damaged Smartcard revoked and replaced as soon as possible. In the case of loss or theft the RA Manager must be informed so that checks may be made to ensure that the Smartcard has not been misused.

When an issued Smartcard becomes unusable or it is lost or stolen the Smartcard certificate must be revoked, as detailed in section **Leavers and Revocation**. Revocation renders the Smartcard useless.

As long as the Smartcard holder's identity can be verified at a face to face meeting a new Smartcard may be issued. Identity will be confirmed by the photograph on their Smartcard or via their Account Recovery Passcode,

- If the identity cannot be verified, the applicant is required to produce documentary evidence to the RA, as detailed in Appendix One.
- If the identity still cannot be verified, the incident is reported to the RA manager. It may be necessary to cancel or revoke the locked NHS Smartcard.

PIN/Pass-code Unlocking/Changing

Users who have forgotten their PIN/Pass-code or suspect that it may be known by another or who have been locked out of CRS Applications because of three failed

login attempts; should report the problem to the RA Team as soon as is practicable by emailing workforce@shsc.nhs.uk.

An RA Agent will then arrange to have the PIN/Pass-code changed with the user. This task must be carried out by a Registration Agent or Sponsor. The Smartcard holder must be present. Their identity will be confirmed by

The photograph on their Smartcard or via their Account Recovery Passcode,

- If the identity cannot be verified, the applicant is required to produce documentary evidence to the RA.as detailed in Appendix One.
- If the identity still cannot be verified, the incident is reported to the RA manager. It may be necessary to cancel or revoke the locked NHS Smartcard.

Record Keeping

All personal data held by the Registration Authority will be protected in accordance with the Data Protection Act (1998). Amongst the measures taken to maintain confidentiality are:

- All documents will be kept in locked and secure storage facilities with access limited to those who have a legitimate use for the information.
- RA Manager and Agents are bound by the requirement to maintain the confidentiality of personal information provided to them as part of the authentication process.
- Sponsors are not required to have sight of any personal identity statements relating to smart card applicants
- The RA will not hold information on applicants other than the minimum requirement for a record of authentication

Requirements for the retention of evidentiary information used for authentications must be fully compliant with the requirements of Health Service Circular HSC 1999/053 – Managing Records in Trust and Health Authorities. (DH Gateway document reference 5130)
Documentation will be kept for 6 years after the applicant leaves the Trust, or until their 70th birthday, whichever is later. Only the summary needs to be kept to age 70. It is the responsibility of the RA Manager to ensure compliance with all aspects of record keeping.

Local Audit

The management and use of Smartcards will be subject to internal and external audit to ensure that national and local policies are being followed.

To ensure compliance with national audit requirements, the RA Manager will produce an annual report which details any changes in the RA Managers and Sponsors assigned to the Trust. This report will be shared with a chosen executive and Trust board.

Specifically, Auditors will look to confirm that:

- Smartcards are handled securely by Users

- RA documents are used and stored appropriately
- Access to CRS Applications and Records is controlled appropriately
- Unused Smartcards are stored safely and appropriate records are kept
- RBAC/PBAC role allocation and de-allocation is performed appropriately
- Random checking of RBAC/PBAC roles with those requested by the sponsor
- Sufficiency of equipment and consumables

The Trust will implement an audit policy to include regular

- Audits on NHS Smartcard use
- Verification that access assigned to individuals is accurate and access is promptly removed which is no longer required
- Verification that individuals are aware of the terms and conditions of NHS Smartcard usage

In accordance with National recommendations Registration Authorities must retain sufficient records to be able to determine, at a later date, the supporting evidence and methods used to verify and validate identity. In particular, all of the following information must be recorded by Registration Authorities for all Certificate Holders registered:

- The identity requirements that were met.
- The unique document numbers of identity documents that contain such numbers.

8. Development, consultation and approval

The policy has been developed as a joint working document between HR and IMST as the overall process within the Trust will be reliant on both departments having strong communication links at all times to ensure correct process.

The document will be reviewed by Policy Governance Group on April 30th 2020 and will be reviewed again once the new Electronic Patient Record has been procured in the 2020/21 financial year.

9. Audit, monitoring and review

Area for Monitoring	How	Who by	Reported to	Frequency
Number of leavers who remain active on the system	Monthly audit	RA Team	RA Manager HROD	Monthly Annually
Number of IR1 forms completed which are linked to smartcard usage.	Quarterly Audit	Health and Safety Team	RA Manager HROD	Quarterly Annually
Number of IR1 forms	Quarterly audit	Health and Safety Team	RA Manager HROD	Quarterly Annually
Internal Audits	Quarterly audits	RA Manager and IG Manager	HROD	Annually
Sponsors confirm that all staff remaining in employment are performing the same duties and have appropriate access levels	Annual review	All Sponsors	RA Manager HROD	Annually Annually

Policy documents should be reviewed every three years or earlier where legislation dictates, or practices change. The policy review date should be no later than March 2023.*

**The current replacement for the Insight programme is underway (although paused due to COVID-19) and the Smartcard project is a dependency for that programme and this policy should be reviewed once the Trust understands what system is due to be procured.*

10. Implementation Plan

Implementation plan is detailed in the section 7 Procedure / Implementation.

11. Dissemination, storage and archiving (Control)

The policy will be made available to all staff and relevant outside bodies and organisations. The policy is available on the Trust's intranet and available to all staff. All policy updates are disseminated out to all staff weekly via the weekly communications update email.

Any and all previous versions must be deleted and replaced with version 2.0. All current policies including this one is stored on the Trust Intranet site under the policies section.

RA Equipment and RA Documentation Storage

All RA Equipment must be stored securely in accordance with the national guidance. Mobile RA Equipment must be adequately protected at all times and not be left unattended. If this is unavoidable, i.e. in the case of emergency, all Smartcards must be removed from the Printer.
RA forms should always be kept separately from the RA Equipment when transporting from site to site in order to ensure data security.

Smartcards should be kept in a lockable unit when not required.

All personal and sensitive non-personal information e.g. RA Forms, Lists of RA Agents and Sponsors held, received or recorded must be adequately protected in accordance with Trust Policies.

All RA forms must be accurately completed and marked with the users UUID number and filed in a locked cabinet. They are to be handled and stored securely at all times with access restricted to RA Agents and HR Staff.

RA Forms will be retained in accordance with the Trusts Information Life Cycle and Records Management Policy.

It is the responsibility of the RA Manager to ensure compliance with all aspects of document storage.

Version	Date added to intranet	Date added to internet	Date of inclusion in Connect	Any other promotion/ dissemination (include dates)
1.1	2015	2015	2015	
2.0	May 2020	May 2020	May 2020	

12. Training and other resource implications

Where individual training needs are identified, the line manger must consult with the Education, Training and Development Team/HR as appropriate.

13. Links to other policies, standards (associated documents)

- Induction Policy
- Grievance and Dispute Procedure
- Policy and Procedure for the Management of Disciplinary Matters– Employment Policies, Section B
- Incident Reporting Policy, Health and Safety Policies
- Informatics Security Policy, Informatics and knowledge Services Policies

14 Contact details

Title	***Name***	***Phone***	***Email***
HR Director	Dean Wilson	0114 22 63960	Dean.wilson@shsc.nhs.uk
HR & Workforce Information Manager	Aimee Hatchman	0114 27 16778	Aimee.hatchman@shsc.nhs.uk
Assistant Deputy Director IMST	Ben Sewell	0114 27 11144	Ben.sewell@shsc.nhs.uk

Privacy, Dignity and Respect
The NHS Constitution states that all patients should feel that their privacy and dignity are respected while they are in hospital. High Quality Care for All (2008), Lord Darzi's review of the NHS, identifies the need to organise care around the individual, 'not just clinically but in terms of dignity and respect'.

As a consequence, the Trust is required to articulate its intent to deliver care with privacy and dignity that treats all service users with respect. Therefore, all procedural documents will be considered, if relevant, to reflect the requirement to treat everyone with privacy, dignity and respect, (when appropriate this should also include how same sex accommodation is provided).

Mental Capacity Act
Central to any aspect of care delivered to adults and young people aged 16 years or over will be the consideration of the individual's capacity to participate in the decision-making process.

Consequently, no intervention should be carried out without either the individuals informed consent, or the powers included in a legal framework, or by order of the Court
Therefore, the Trust is required to make sure that all staff working with individuals who use our service are familiar with the provisions within the Mental Capacity Act. For this reason, all procedural documents will be considered, if relevant to reflect the provisions of the Mental Capacity Act 2005 to ensure that the interests of an individual whose capacity is in question can continue to make as many decisions for themselves as possible.
Indicate How This Will Be Achieved.
All individuals involved in the implementation of this policy should do so in accordance with the Guiding Principles of the Mental Capacity Act 2005. (Section 1)

Appendix A

Equality Impact Assessment Process and Record for Written Policies

Stage 1 – **Relevance** - Is the policy potentially relevant to equality i.e. will this policy potentially impact on staff, patients or the public? This should be considered as part of the Case of Need for new policies.

NO – No further action is required – please sign and date the following statement.

I confirm that this policy does not impact on staff, patients or the public.

Stage 2 Policy Screening and Drafting Policy - Public authorities are legally required to have 'due regard' to eliminating discrimination, advancing equal opportunity and fostering good relations in relation to people who share certain 'protected characteristics' and those that do not. The following table should be used to consider this and inform changes to the policy (indicate yes/no/ don't know and note reasons). Please see the SHSC Guidance and Flow Chart.

SCREENING RECORD	Does any aspect of this policy or potentially discriminate against this group?	Can equality of opportunity for this group be improved through this policy or changes to this policy?	Can this policy be amended so that it works to enhance relations between people in this group and people not in this group?
Age	**No**	The policy is consistent in its approach to the RA function and provision of smart cards regardless of the employee's age.	
Disability	**No**	The policy is consistent in its approach to the RA function and provision of smart cards regardless of the employee's disability	
Gender Reassignment	**No**	The policy is consistent in its approach to the RA function and provision of smart cards regardless of the employee's gender.	
Pregnancy and Maternity	**No**	The policy is consistent in its approach to the RA function and provision of smart cards regardless of the employee's pregnancy or maternity.	
Race	**No**	The policy is consistent in its approach to the RA function and provision of smart cards regardless of the employee's race.	

Religion or Belief	**No**	The policy is consistent in its approach to the RA function and provision of smart cards regardless of the employee's religion or belief.	
Sex	**No**	The policy is consistent in its approach to the RA function and provision of smart cards regardless of the employee's sex.	
Sexual Orientation	**No**	The policy is consistent in its approach to the RA function and provision of smart cards regardless of the employee's sexual orientation.	
Marriage or Civil Partnership	**No**		

Appendix B

REGISTRATION AUTHORITY IDENTITY DOCUMENTS

In order to check your identification and allow you access to the NHS Care Records Service with a smartcard, please provide documentation in accordance with the list below, and in either of the following combinations;

a) Two forms of photographic ID and one document confirming your address.

OR

b) One form of photographic ID and two documents confirming your address.

If for any reason you are unable to provide all of the documentation specified, or if you are unsure as to whether your documentation is acceptable, please contact the RA team on workforce@shsc.nhs.uk . If you attend your smartcard appointment with incorrect documentation you will not be issued with a smartcard.

Acceptable photographic identification is;

- UK (Channel Islands, Isle of Man or Irish) passport or EU/other nationalities
- passport
- Passports of non-EU nationals and other valid evidence relating to their immigration status and permission to work*
- UK full or provisional photo-card driving licence **(must include paper counterpart)**
- EU/other nationalities full photo-card driving licence (valid up to 12 months up to the date of when the individual entered the UK)
- Biometric Residence Permit (formerly known as identity cards for foreign nationals)*
- HM Armed Forced Identity Card
- ID Card carrying the PASS accreditation logo (UK and Channel Islands), for example a UK Citizen ID Card. This card can be applied for by residents of the UK and is verifiable with similar security marks to UK passports and driving licences.

Any other document, for example organisation ID cards, will not be accepted as photographic personal identification. If photographic ID cannot be provided, please contact the RA team by email on smartcards@shsc.nhs.uk for advice.

Acceptable confirmation of address documents are;

- Utility bill (gas, water, electricity or land-line telephone), or a certificate from a utility supplier confirming the arrangement to pay for the services on pre-payment terms at a fixed address. Must be original documentation and not downloaded from the internet. Utility providers will provide official statements on request. More than one utility bill may be accepted if these are from two different suppliers and utility bills in joint names are also permissible*
- Local authority tax statement (i.e. council tax)**
- UK full or provisional photo-card driving licence (must include paper counterpart); or a full old-style paper driving licence (if not already presented as a personal ID document).

- Old style provisional driving licences are not acceptable
- Most recent HM Revenue & Customs tax notification (i.e. tax assessment, statement of account, notice of coding)** a P45 or P60 is not acceptable
- Financial statement (for example, bank, building society, credit card or credit union statement) containing current address* Must be original documentation and not downloaded from the internet. Financial institutions will provide official statements on request.
- Mortgage statement from a recognised lender**
- Local council rent card or tenancy agreement*
- Benefit statement, book or card; or original notification letter from Department of
- Work and Pensions (DWP) confirming the rights to benefit (for example, child allowance, pension)**
- Confirmation from an electoral register search that a person of that name lives at the claimed address**.

* = *Documents must be dated within the last 3 months*
** = *Documents must be dated with the last 12 months*

If you intend to use two confirmations of address documents, please ensure they are from two separate organisations.

To be issued with a card you must also give your National Insurance Number. Proofs of this is not required, but please ensure that you know your NI number as it must be recorded on the system for a card to be produced.

Appendix C

What to do if no acceptable photographic personal identification documents are available:

If an individual seems genuinely unable to provide any acceptable photographic personal identification, then employers should request each of the following:

- two forms of non-photographic personal identification
- two documents confirming their address
- a passport-sized photograph of themselves.

All documents must be from a different source and **photographs must be endorsed on the back** with the signature of a 'person of standing' in their community, who has known them for at least three years. A 'person of standing' may be a magistrate, medical practitioner, officer of the armed forces, teacher, lecturer, lawyer, bank manager or civil servant.

The photograph should also be accompanied by a signed statement from that person, indicating the period of time that the individual has been known to them and the name, address and telephone number of the person signing the statement.

List of acceptable confirmation of address documents

Acceptable documents for confirmation of address include:

- utility bill (gas, water, electricity or phone), or a certificate from a utility supplier confirming the arrangement to pay for the services on pre-payment terms at a fixed address. More than one utility bill may be accepted if these are from two different suppliers and utility bills in joint names are also permissible*
- local authority tax bill (i.e. council tax)**
- UK full or provisional photo-card driving licence (must include paper counterpart); or a full old-style paper driving licence (if not already presented as a personal ID document). Old style provisional driving licences are not acceptable
- most recent HM Revenue & Customs tax notification (i.e. tax assessment, statement of account, notice of coding). A P45 or P60 is not acceptable**
- financial statement (e.g. bank, building society, store card, credit card or credit union statement) containing current address*
- mortgage statement from a recognised lender**
- local council rent card or tenancy agreement*
- benefit statement, book or card; or original notification letter from Department of Work and Pensions (DWP) confirming the rights to benefit (eg child allowance, pension)**
- insurance certificate**
- UK court claim form**
- TV licence**
- confirmation from an electoral register search that a person of that name lives at the claimed address*.

Documents marked with an '*' must be dated within the last three months. (Unless there is a good reason for it not to be, eg, clear evidence that the person was not living in the UK for three months or more). These documents must contain the name and address of the applicant.
Documents marked with '**' must be dated within the last 12 months.

List of acceptable non-photographic proof of personal identification documents

Acceptable non-photographic documents include:

- full UK birth certificate – issued within 12 months of birth
- UK full old-style paper driving licence. Old-style provisional driving licences are not acceptable
- residence permit issued by the Home Office to EU Nationals on inspection of own-country passport
- adoption certificate
- marriage/civil partnership certificate
- divorce/annulment or civil partnership dissolution papers
- deed poll certificate
- police registration document
- certificate of employment in HM Forces
- benefit statement, book or card, or original notification letter from the Department of Work and Pensions (DWP) confirming legal right to benefit (e.g. child allowance, pension)**
- most recent tax notification from HM Revenue and Customs (ie. tax assessment, statement of account, notice of coding). A P45 or P60 is not acceptable**
- UK firearms certificate
- Application Registration Card (ARC) issued to people seeking asylum in the UK (or previously issued standard acknowledgement letters, SAL1 or SAL2 forms)
- GV3 form issued to people who want to travel in the UK without valid travel documents
- Home Office letter IS KOS EX or KOS EX2
- building industry sub-contractor's certificate issued by HM Revenue and Customs
- grant letter or student loan agreement from a Local Education Authority.

When appointing someone who has recently left school or further education, in addition to photographic personal identification, the following three documents can be requested as sufficient proof of their identity:

- full UK birth certificate – issued within 12 months of birth
- National Insurance (NI) number card or proof of issue of an NI number (this will also be a HR requirement for employment)
- certificate of educational qualifications (certificates must be originals from the school/university/awarding body).

Taken from the NHS Employment Check Standards: Identity Checks (July 2013)