

The Newcastle upon Tyne Hospitals NHS Foundation Trust

Registration Authority Policy

Effective: October 2011

Review: September 2012

1. Introduction

The process of gaining access to National Programme applications e.g. Choose & Book, Secondary User Services (SUS), Summary Care Record and SystemOne, is called National Programme Registration. To enable healthcare professionals to access national applications, registration onto the national spine needs to take place. All the National applications use a common security and confidentiality approach. This is based upon the NHS professional's organisations roles, areas of work and business function.

The primary method by which users will be enabled to access a national application is via a Smartcard issued during the Registration Process. Once an applicant has been successfully registered they will have a user ID, pass-codes and Smartcard which will permit their access to the appropriate applications and information. The process is operated at a local level by a Registration Authority (RA) which is required to conform to the National Registration Policy and Practices identified below.

Within the Trust, access to local systems and applications are also managed through a single sign-on process (Smartcard access) and uses the security aspects of the national database to manage the smartcards. This means that all staff that require access to either national or local electronic information systems must be processed through the RA procedures.

Unauthorised access, modification, transfer, disclosure, or deletion of computer held records are criminal offences under the Computer Misuse Act 1990 and make the offender liable to a fine, or five years imprisonment or both. These offences constitute gross misconduct and may result in summary dismissal of the offender. Unauthorised access, modification, transfer, disclosure, or deletion of manual records will attract similar disciplinary action as may misuse of the Trusts' E-mail and Internet services.

This document describes procedures for the operation of the Registration Authority (RA) within the Trust.

2. Legislation

The Trust is obliged to appoint a Registration Authority to manage the distribution and use of Smartcards.

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://www.National.nhs.uk/implementation/>)
- Registration Policy and Practices for Level 3 Authentications (available from <http://www.National.nhs.uk/implementation/>)
- The NHS Confidentiality Code of Practice (www.dh.gov.uk)

- NCRS Acceptable Use Policy, Terms and Conditions (available from <http://nww.National.nhs.uk/implementation/>)

The procedures covered in this document are the local support procedures necessary to support the National Policies and Procedures:

- Identification and Appointment of RA Team Members
- Registration of RA Manager
- Registration of RA Agents
- Registration of Sponsor
- Registration of National Application Users
- Management of National Application Users
- Management of RA/User Smartcards
- Management of RA/User PIN/Pass-codes
- Management of RA/User Profiles

3. Scope

It is intended that this document is used by the following people:

- Trust Board Members
- All users of the Trust RA Service.
- Trust Human Resources staff.
- Trust IT Services staff.
- Trust Confidentiality Specialists including Caldicott Guardians.

4. Roles and Responsibilities

4.1 The Registration Authority (RA)

RA is an official or committee within the Trust with appropriate organisational authority that is responsible for ensuring all aspects of registration services and operations are performed in accordance with national policies and procedures (See section 1). They are responsible for providing arrangements that will ensure tight control over the issue and maintenance of electronic Smartcards, whilst providing an efficient and responsive service that meets the needs of the users.

The Registration Authority has the following responsibilities:-

- Ensuring that the National Registration processes are adhered to in full as identified in NATIONAL-NCR-DES-0294.02 Registration Policy and Practices for Level 3 Authentications, NATIONAL-FNT-IMD-IME-0182.02 Registration Authorities Setup and Operation and this document
- Ensuring that documentation either paper or electronic forms are appropriately used
- 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 their organisational responsibilities
- Ensuring that the RA team members are adequately trained and familiar with the local and national RA processes
- Electronic forms managed through the ESR interface will be used to identify and audit users and changes.

- Ensure RA members are familiar with and understand Registration Policy and Practices for Level 3 Authentications - NATIONAL-NCR-DES-0294.02, NATIONAL-FNT-IMD-IME-0182.02 Registration Authorities Setup and Operation and this document
- Notification of the creation and revocation of RA managers (including their e-mail address) by sending an e-mail to ramanagers@National.nhs.uk
- Ensuring that there are sufficient Smartcards and Smartcard issuing and maintenance equipment for the organisation. Note: see NATIONAL-FNT-IMD-IMPPOCP-0001.01RA Hardware Ordering Process

The Trust Registration Authority is made up of the following personnel:

- Registration Authority Managers
- Registration Sponsors
- Registration Agents

4.2 Registration Authority Managers

4.2.1 The RA Manager is selected by the Trust Executive and is responsible for the set up and day to day running of the Trust RA service. The Trust has a number of RA managers:

- **Head of Information Governance & IT Security** who will take responsibility for audit of users and strategic RA
- **Head of Staff Engagement** who will manage operational process
- There are several other Managers based in HR including Medical Staffing and Nurse Bank who manage the process on a daily basis

The RA Managers will ensure that all RA procedures are carried out in accordance with local and national policy.

4.3 Registration Agents

Registration Agents are responsible to the RA Manager for ensuring that the national and local processes are followed and for the accurate input of information onto the National Spine User Directory and Card Management System. RA Agents may be from HR including Medical Staffing or IT. RA staff within HR will register new users and issue cards. They will be responsible for changes to designation and revocation of cards for leavers. The management of these functions is through the ESR link or by direct user interface.

RA staff within IT will manage card recertification or unlocks.

Registration Agents will ensure that all inter-Trust agreements are followed and adhered to. All incidents, misuses, anomalies, and problems will be reported to the RA Manager

5. Services

The services available will be:

- User Registration
For new starters this will occur when ID badge is issued on first day of employment.
- Role Profile maintenance
 - adding Role Profiles
 - changing Role Profiles
 - deactivating Role Profiles
- Revocation and cancelling of Smartcards

- User Suspension
- PIN/Pass-code resetting
- Smartcard renewal and exchange

The above services will be available during the Trust Registration Service Core hours, 08:00 to 17:30 Monday to Friday for Non Medical & Dental staff and 8.30- 17.00 for Medical & Dental staff, excluding public holidays. The following reduced set of services, will be available at other times accessible via the IT Service desk: Tel 21000

- PIN/Pass-code resetting
- Recertification of Smartcards
- Revocation

Registration Services outside of core hours should be considered as emergency only. They should only be requested when waiting until core hours would be detrimental to patient care or confidentiality.

6. Training

All Trust RA Members will have sufficient training to carry out their RA tasks in accordance with national policies and procedures. They will be individuals capable of trust as they will be handling sensitive information covered by The Data Protection Act. They will be key players in ensuring the NHS Code of Confidentiality and NATIONAL-FNT-TO-IG-0052.01 NCRS Acceptable Use Policy, Terms and Conditions (<http://www.National.nhs.uk/implementation/>) is followed.

7. 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 Procedure, to the RA Manager.

Examples of incidents are:

- Smartcard or application misuse.
- Smartcard theft.
- Non-compliance of local or national RA policy.
- Any unauthorised access of National applications.
- Any unauthorised alteration of patient data.

The RA manager will consider all incidents reported to them. Any incidents considered significant will be escalated to the Trust Board, HR, and/or the Trust Caldicott Guardian depending on the nature of the incident. A major breach of security will also be reported by the RA manager locally or nationally to the appropriate bodies as required.

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 Board and/or Caldicott Guardian will consider incidents reported to them and decide whether Trust systems or working practices should be reviewed as a result.

Incidents involving breaches of security or demonstrate that a User may not be considered trustworthy should also be reported to HR and Caldicott Guardian by the RA Manager for consideration of whether any formal action under the Disciplinary Procedure is necessary. HR will advise which other members of staff need to be involved (e.g. line manager, IT Manager).

Failure of or unavailability of national applications should be reported in the first instance to the IT service desk Ext 21000 who will escalate the problem to the local RA or the national helpdesk.

8. Processes and procedures

The Trust will ensure that processes supporting the identification, registration and management of staff will be integrated with other Trust processes as appropriate. (See *appendices*)

9. Management and use of RA Equipment

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

10. Management of National Application Users

Management of the national application users is through RA forms. All RA forms are electronic format and will be managed through the ESR/ UIM interface.

10.1 Lost or Damaged Smartcards

Lost and damaged Smartcards should be reported to the RA Team as soon as is practicable by using the IT Service desk on Ext 21000. Once notified that a Smartcard has been lost or damaged IT department based RA agents will arrange to have the lost/damaged Smartcard revoked and replaced (see below) 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. Ref: Section 12 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 with an RA agent a new Smartcard may be issued.

If there is any difficulty verifying the user's identity, the user's sponsor must be contacted and the users' identity verified. It is vital that the sponsor's identity can be relied upon when contacting them to verify the user's identity.

10.2 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 national applications because of three failed login attempts; should ask the sponsor to unlock the card or reset the PIN. If there is still a problem it should be reported to the RA Team as soon as is practicable by using the IT Service desk on Ext 21000
The Smartcard holder must be physically present for a reset or unlock.

10.3 Recertification

All certificates on smart cards expire every two years. A 30 day warning notification will be given when an individual whose certificates are about to expire log onto the system prompting the individual to follow the necessary steps to recertify their own card.

Any problems relating to recertification should be directed to the Service desk.

10.4 Profiles

What a user is able to access is based on the information in the profile. Whenever there is a temporary or permanent change in the way a person works, a review of the person's national application access must be carried out. If there are significant changes to the staff member's role the relevant role profile on the National Spine User Database must be requested via a suitable sponsor. Examples of changes that would necessitate such changes are changes to a person's:

- Job Title
- Access requirements
- Department
- Site(s)
- Work Group

Where vacancies arise the vacant post must be reviewed and the level of access to national systems must be identified on the RCG application form. Once the post is agreed the HR department will be notified of the appropriate job title to be allocated to the successful candidate to ensure correct access is given. This will be indicated on the RCG minutes.

Where the user is leaving the NHS please refer to section 12 Leavers and Revocation.

11. Leavers and Revocation

When an individual leaves the Trust and this is recorded in ESR the ESR/UIM interface ensures that the card is revoked.

There are other 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. 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 Manager
The relevant Sponsor(s)
The RA User

Revocation renders the Smartcard useless.

Revocation can only be carried out by Registration Managers and Agents on the request of HR.

12. Locums, Agency and Bank Personnel

Temporary staff may need access to national 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 fill the role
- some temporary staff could already be enrolled 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 national application needed to be accessed
- locum staff coming into the Trust as out of hours support are issued with temporary smartcard access to local applications but the locum profile has no access to national applications. The temporary cards are managed by A&E staff and Patient Services Co-ordinators.
- Local support processes for National Application Users who need support should contact the IT service desk on Ext 21000

13. 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. Specifically, Auditors will look to confirm that:

- Smartcards are handled securely by Users
- Access to National Applications and Records is controlled appropriately
- Unused Smartcards are stored safely and appropriate records are kept
- RBAC role allocation and de-allocation is performed appropriately
- Random checking of RBAC roles with those requested by the sponsor

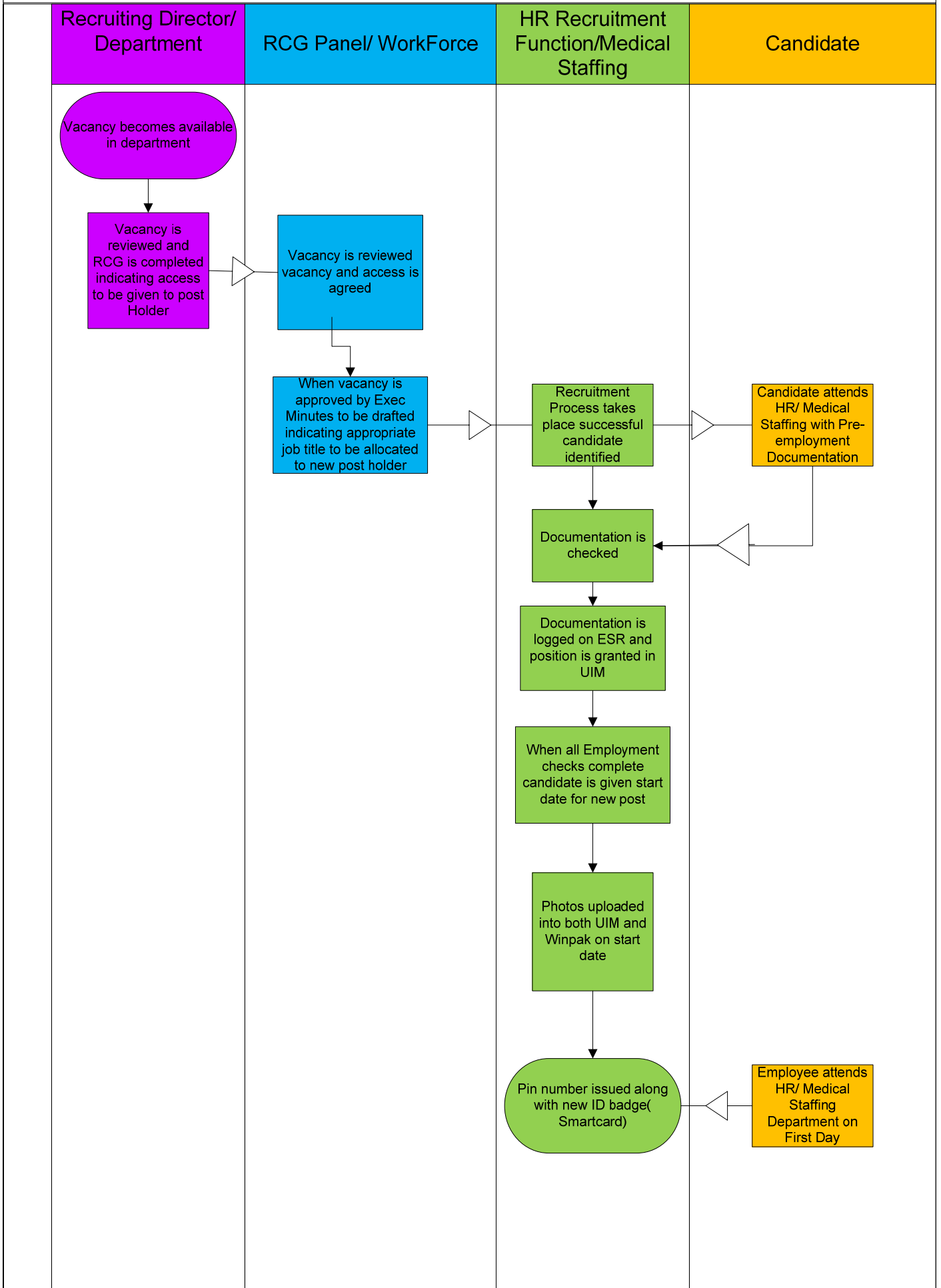
To aid audit the following records will be maintained:

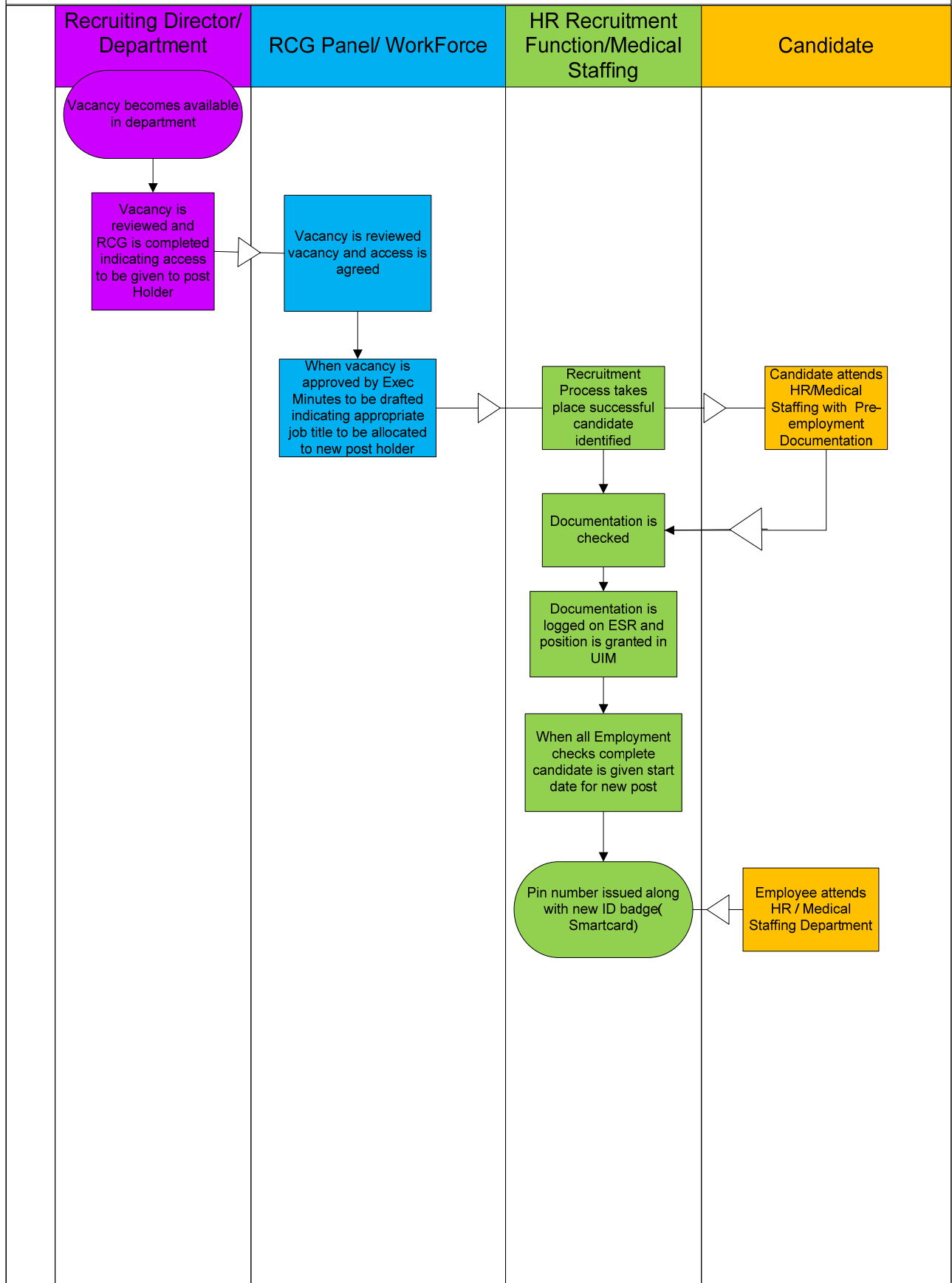
- the number of Smartcards held
- details of Smartcards issued
- The number and location of smartcard printers.

14. Review

This policy will be reviewed by Head of Staff Engagement and Head of Information Governance on an annual basis or as a result of any legislation changes.

Author: Head of Staff Engagement and the Head of Information Governance.





**THE NEWCASTLE UPON TYNE HOSPITALS NHS FOUNDATION TRUST
IMPACT ASSESSMENT – SCREENING FORM A**

This form must be completed and attached to any procedural document when submitted to the appropriate committee for consideration and approval.

Policy Title:	Registration Authority	Policy Author:	Mrs Julie Anderson, Head of Staff Engagement
		Yes/No?	You must provide evidence to support your response:
1.	Does the policy/guidance affect one group less or more favourably than another on the basis of the following: (* denotes protected characteristics under the Equality Act 2010)		Policy applies to all employees of the Trust. It is underpinned by the Trust's overriding policy on equal opportunities
	• Race *)
	• Ethnic origins (including gypsies and travellers))
	• Nationality)
	• Gender *) see above
	• Culture)
	• Religion or belief *)
	• Sexual orientation including lesbian, gay and bisexual people *)
	• Age *)
	• Disability – learning difficulties, physical disability, sensory impairment and mental health problems *)
	• Gender reassignment *)
	• Marriage and civil partnership *)
2.	Is there any evidence that some groups are affected differently?		There is no evidence to support any group was affected differently
3.	If you have identified potential discrimination which can include associative discrimination i.e. direct discrimination against someone because they associate with another person who possesses a protected characteristic, are any exceptions valid, legal and/or justifiable?		n/a
4(a).	Is the impact of the policy/guidance likely to be negative? <i>(If "yes", please answer sections 4(b) to 4(d)).</i>		No
4(b).	If so can the impact be avoided?		n/a
4(c).	What alternatives are there to achieving the policy/guidance without the impact?		n/a
4(d)	Can we reduce the impact by taking different action?		n/a

Comments:	Action Plan due (or Not Applicable):
------------------	---

Name and Designation of Person responsible for completion of this form: Mrs Julie Anderson Date:.....12 September 2011.

Names & Designations of those involved in the impact assessment screening process:..... Employment Polices and Procedures Consultation Group.....

_(If any reader of this procedural document identifies a potential discriminatory impact that has not been identified on this form, please refer to the Policy Author identified above, together with any suggestions for the actions required to avoid/reduce this impact.)