


**TRUST POLICY FOR REGISTRATION AUTHORITY AND INTEGRATED IDENTITY MANAGEMENT (IIM)**

<b>Reference Number</b>  POL-HR/1653/13	<b>Version:</b> 2.1		<b>Status:</b> Final	<b>Author:</b> Greg Chambers  <b>Job Title:</b> Workforce Systems Lead
<b>Version / Amendment History</b>	<b>Version</b>	<b>Date</b>	<b>Author</b>	<b>Reason</b>
	1.0	January 2013	Rachel Loveridge	Combined with the Trust Policy and Procedures for Registration Authority (Smartcard Access) and integration of RA/Workforce Management functions following the activation of the ESR and IIM/UIM Interface
	1.1	Sept 2015	Sylvia Allen	As part of the IIM replacement project from UIM to CIS, RA Policy updated to ensure it is clear and aligned with the Care Identity Services Application
	1.2	July 2018	Adam Race	Derby Policy unified for UHDB
	2.0	July 2019	Greg Chambers	Major Policy Update
	2.1	Dec 2022	Greg Chambers	Minor Amendments
<b>Intended Recipients:</b> All Trust staff, visiting staff from other organisations, employees or temporary employment agencies and third-party users and contractors				
<b>Training and Dissemination:</b> Available on Trust Intranet				
<b>To be read in conjunction with:</b> Trust Recruitment Policy, Trust Policy and Procedure for Information Governance; Trust Policy and Procedure for Data Protection and Dealing with Confidential Information; Trust Policy and Procedure for Information Technology and Cyber Security.				

<b>In consultation with and Date:</b> Workforce Policy Review Group (WPRG) Oct 2019; Trust Joint Partnership Forum (TJPF) Nov 2019; Joint Local Negotiating Committee (JLNC) Nov 2019; Workforce Review Group (WRG) November 2019; Trust Operational Group (TOG) February 2020, consulted Head of Information Governance December 2022 ; Information Governance Steering Group	
<b>EIRA stage One</b>	Completed Yes
stage Two	Completed Not applicable
<b>Approving Body and Date Approved</b>	Approved by the Trust Delivery Group – 04 February 2022.  Minor Amendments approved by the Interim Executive Medical Director – 15.12.2022
<b>Date of Issue</b>	December 2022
<b>Review Date and Frequency</b>	December 2025 then every 3 years
<b>Contact for Review</b>	Workforce Systems Lead
<b>Executive Lead Signature</b>	 James Crampton - Interim Executive Medical Director

## Contents

<b>1. Introduction</b>	<b>4</b>
<b>1.1 Registration Authority (RA)</b>	<b>4</b>
<b>1.2 Integrated Identity Management (IIM)</b>	<b>4</b>
<b>2. Purpose and Outcomes</b>	<b>5</b>
<b>3. Definitions</b>	<b>5</b>
<b>4. Key Responsibilities/Duties</b>	<b>6</b>
<b>5. Current Processes</b>	<b>7</b>
<b>5.1 Trust Staff</b>	<b>8</b>
<b>5.2 Position Based Access Control (PBAC)</b>	<b>8</b>
<b>5.3 Amendment to an existing Access Control Position (ACP)</b>	<b>8</b>
<b>5.4 Removal of an ACP</b>	<b>8</b>
<b>5.5 New ACP</b>	<b>9</b>
<b>5.6 ESR Position Linking</b>	<b>9</b>
<b>5.7 Amendment to an ESR Position</b>	<b>9</b>
<b>5.8 Removal of an ESR Position</b>	<b>10</b>
<b>5.9 New ESR Position</b>	<b>10</b>
<b>5.10 Personal Information Management</b>	<b>10</b>
<b>5.11 Automated Addition and Revocation of NHS CRS Access</b>	<b>10</b>
<b>5.12 CIS</b>	<b>10</b>
<b>5.13 External Staff</b>	<b>10</b>
<b>5.14 Keep In Touch Days</b>	<b>11</b>
<b>5.15 Non-ESR Staff</b>	<b>11</b>
<b>5.16 Change of Access</b>	<b>11</b>
<b>5.17 Leavers</b>	<b>11</b>
<b>5.18 Non ESR Staff</b>	<b>11</b>
<b>5.19 RA Agent configuration in ESR</b>	<b>12</b>
<b>5.20 NACS/ODS Codes in ESR</b>	<b>12</b>
<b>5.21 RA Notifications in ESR</b>	<b>12</b>
<b>5.22 RA URPs in ESR</b>	<b>12</b>
<b>5.23 RA Dashboard</b>	<b>12</b>
<b>5.24 Equipment and Maintenance</b>	<b>13</b>
<b>5.25 Training</b>	<b>13</b>
<b>6. Monitoring Compliance and Effectiveness</b>	<b>13</b>
<b>6.1 Internal Audit</b>	<b>13</b>
<b>Appendix 1</b>	<b>14</b>
<b>1.1 System Processes</b>	<b>14</b>

# TRUST POLICY FOR REGISTRATION AUTHORITY AND INTEGRATED IDENTITY MANAGEMENT

## 1. Introduction

### 1.1 Registration Authority (RA)

The Registration Authority was introduced by the Department of Health in March 2005. This document lays out the RA Policy requirements and is based on the original DH Gateway document (reference number 6244) 'Registration Authorities: Governance Arrangements for NHS Organisations', the NHS Care Record Guarantee, the Data Protection Act 2018 and requirements contained in the NHSD RA Process Guidance together with Data Security and Protection Toolkit requirements in relation to Registration Authorities. All organisations that run a local Registration Authority do so on a delegated authority basis from NHSD.

The Trust has a duty to comply with Information Governance legislation and regulation. An important element of this is to ensure that staff members comply with the Terms and Conditions associated with them being issued with an NHS Smartcard and having access to NHS applications and services. The Trust must also comply with its Information Governance responsibilities for effective staff registration processes, establishing business processes and arrangements to satisfy its RA obligations and to ensure that access, profiling, issue, revocation and management of Smartcards is appropriate. The Trust is responsible for establishing its own RA Service. The Trust's RA responsibilities require assurance that associated equipment such as computers, Smartcard Readers and Smartcards are held in sufficient quantity, fit for purpose and protected.

### 1.2 Integrated Identity Management (IIM)

In 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 organisation's RA to verify an individual's identity before allowing access to NHS Care Records Service (NHS CRS) applications.

Combining these two parallel activities into a single Integrated Identity Management (IIM) process has proven to deliver significant benefits through Workforce Management/RA process integration. The move to Position Based Access Control (PBAC) is supported by the new software applications described below (CIS and ESR-CIS Interface).

IIM significantly improves access control to NHS CRS systems containing person identifiable information through revised business processes and the introduction of two new software applications:

- **Care Identity Service (CIS)** is the registration software to manage NHS CRS access control and facilitate the Interface to ESR. CIS uses electronic forms and digital signatures thereby removing the need for paper-based workflow. The implementation of CIS requires no data to be migrated. Access control in CIS is facilitated using NHS CRS Access Control Positions (ACP) defined by the Position Based Access Control methodology which is therefore a pre-requisite to its implementation.
- **ESR-CIS Interface** can be used to link staff records in ESR to user records in NHS CRS in order to remove duplication and to drive access control based on the job that a person holds. Workforce Management functions currently update ESR when changes are made regarding an employee's assignment to an established position. Where a position is linked to an NHS CRS ACP, the ESR interface will be triggered by such changes and will automatically update an

individual's access rights to NHS CRS compliant systems to reflect the requirements of their new position or status.

Based on the significant benefits and improved Governance, the Trust elected to implement the ESR-CIS Interface which was activated on 14th March 2011 alongside CIS. To realise further benefits the Trust has reviewed processes/procedures and explored integration opportunities, for both directly and externally employed staff, in the following areas:

- New Starters
- Managing HR changes (e.g. an employee changing job role or department)
- Leavers.

This document is the **Trust Policy for Registration Authority and Integrated Identity Management** and is relevant to both Registration Authority and ESR users to ensure that any changes made in ESR and CIS, which have a direct impact on the ESR-CIS Interface, are considered and reviewed in accordance with the continued functionality of the software.

## 2. Purpose and Outcomes

The purpose of this document is to outline the agreed processes required to manage the distribution and use of Smartcards and to support and maintain the ESR Interface to CIS on an on-going basis. The document will also provide guidance to ensure that relevant applications continue to be operated safely and efficiently through future developments. The document is not intended to be an exhaustive review of all Workforce Management/RA processes and procedures but rather will focus on following key elements:

### For employed staff

- New starter setup (from acceptance of offer of employment)
- Managing changes to person details, assignments and positions
- Leaver process
- Access control.

### For externally employed staff (requiring access to NHS CRS Applications)

- Registration
- Access control
- Managing changes to person details/access
- Leaver process.

The intended audience of this document are those staff situated within the RA functions and the Workforce Management, Work Structures and Recruitment functions.

## 3. Definitions

**e-GIF Level 3:** Security standards for access to government systems. e-GIF (Government Interoperability Framework) Level 3 refers to policies and standards to enable information to flow seamlessly across the public sector and provide citizens and businesses with better access to public services.

**NHS Digital (NHSD):** NHSD is the national provider of information, data and IT systems for commissioners, analysts and clinicians in health and social care. NHSD is an executive non-departmental public body, sponsored by the Department of Health.

**Care Identity Service (CIS):** NHSD transitioned to the new CIS in February 2015. CIS is the system that manages Smartcard access for over 900,000 health and care workers.

**Data Security and Protection Toolkit:** The DSPT is a performance tool produced by NHSD for the Department of Health. It draws together legal rules and central guidance and presents them in one place as a set of IG requirements. These requirements ensure that organisational processes and procedures are in place to meet an organisation's responsibility to be a Registration Authority and to ensure that NHS Smartcard users comply with the Terms and Conditions of use.

**NHS CRS:** The NHS Care Records Service helps NHS organisations in England to store patient health care records on computers that link information together quickly and easily. An NHS CRS Smartcard gives a user access to the NHS CRS and other National applications such as Choose and Book and the Electronic Prescription Service.

**NHS CRS Smartcard:** A plastic card containing an electronic chip (like a chip and PIN credit card) that is used to access the NHS CRS along with a Passcode. The chip does not contain any personal information. The combination of the NHS CRS Smartcard and Passcode together provide high levels of security and confidentiality.

**Electronic Staff Record:** The Electronic Staff Record (ESR) is an Oracle based human resources and payroll database system used by the National Health Service (NHS) in England and Wales to manage the payroll of NHS staff members.

**Registration Authority:** The Registration Authority (RA) is an official or committee within the Trust with appropriate organisational authority 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 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.

#### **4. Key Responsibilities/Duties**

An overview of the individual, departmental and committee responsibilities.

**Registration Authority Manager:** The RA Manager is responsible for ensuring staff identification meets e-GIF3 standards before issuing Smartcards.

**IT Service Desk Manager:** The IT Service Desk Manager is responsible for the set up and day to day running of the Registration Authority Service, which must be carried out in accordance with local and national policies.

**Workforce Systems Manager:** The Workforce Systems Manager is the Trust lead and Information Asset Owner for ESR and other electronic workforce systems.

**Registration Agents:** The Registration Agents are responsible to the Registration Authority Manager for ensuring that the national and local processes are followed and for the accurate input of information on RA forms onto the Spine User Directory and CIS. Registration Agents ensure that all inter-trust agreements are followed and adhered to.

**Workforce Review Group / Committee** in place at the time, is chaired by the Executive Director of People and Organisational Development and reports to the People Committee. The group is attended by representatives from Finance, IT, Learning & Education and Divisional Management teams and provides strategic and directorial support to the Workforce Systems Delivery Group.

**Workforce Systems Delivery Group:** The Workforce Systems Delivery Group is the operational group appointed to ensure that workforce systems tasks and project actions are completed in line with the project plan.

**Caldicott Guardian:** The appointed Caldicott Guardian must approve all procedures that relate to the use of patient and service-user information and is responsible for enabling appropriate information sharing.

**Senior Information Risk Owner:** The SIRO is responsible for ownership of information risk across the Trust. The SIRO acts as advocate for information risk on the board and provides written advice to the accounting officer on the content of their Statement of Internal Control in regard to information risk.

**Information Governance Steering Group:** The Information Governance Steering Group is chaired by the Caldicott Guardian and reports to the IT Project Steering Group. The group is attended by the SIRO and representatives from IT Services, Information Services, Records Management, Business Development, Clinical Governance and Divisional Management Teams. Any information security issues will be highlighted here for relevant assessment and action.

**Trust Information Governance Group:** The Trust Information Governance Group ensures compliance with Information Governance guidance and promotes and implements best practice initiatives among the IG Leads who work across the Trust. The Group also monitors and reacts accordingly to incidents and meets deadlines concerned with the DSP Toolkit.

## 5. Current Processes

All of the processes identified in this document are the solutions that have been identified and established within the Trust. These will be closely monitored, maintained and adhered to by the intended audience (Workforce Management, Work Structures, RA and Recruitment) to ensure that the organisation maximises the benefits of the ESR interface to CIS to drive the strategic approach to IIM by fully utilising the relevant components including:

- Workforce Management/RA process integration;
- Position Based Access Control;
- ESR Position Mapping and Linking;
- Automated Granting and Revocation of NHS CRS Access rights;
- Recording Identity Checks once in ESR thereby eliminating the duplication of effort.

This will also include the regular review and maintenance of various elements such as Notifications, Organisation Data Service (ODS) Codes and NHS CRS Sponsors' requirements within ESR.

### **5.1 Trust Staff**

As part of the recruitment process, the appointing manager confirms identity, and this information is recorded within ESR by the RA Agents in the Recruitment Team in Workforce Management.

The ESR person record is then associated to the NHS CRS user record to ensure that the relevant NHS CRS Access is assigned to the new starter.

The RA function at the Trust operates a system whereby, staff requiring an NHS CRS Smartcard for the purpose of their role, can visit the IT Service Desk within the advertised times. At this point ID is verified, the staff information is entered directly into ESR and the photograph is taken prior to the Smartcard being produced.

### **5.2 Position Based Access Control (PBAC)**

The Trust has reviewed all of the NHS CRS Access used within the organisation and has developed the ACPs by reviewing existing access and cleansing workforce data in ESR.

It is expected that these ACPs will be reviewed either on an ad-hoc basis when a request has been made or on an annual basis to ensure that the current requirements are still valid. Any adjustments will be processed using the relevant options as stated below.

### **5.3 Amendment to an existing Access Control Position (ACP)**

It is likely that the Trust RA staff will receive a notification to amend an existing ACP via four separate methods:

- A request from an existing user/sponsor
- Identification of amendment through the review process
- Notification from a supplier that an amendment is required
- Trust Acquisitions or Mergers.

Whatever method is used for requesting the change, the process for amendment will still follow the authorisation process that has already been established within the Trust. Therefore, the suggested, or requested, change will need to be approved by the Information Governance Action Group before the amendment is made to the ACP.

If the request for change is denied the person that made the request will be notified of the outcome and this, in turn, could then determine whether a new ACP is created.

It is necessary to ensure that any changes are documented and included within the CIS Position Document and Mapping spreadsheet before it is resubmitted for approval by the Information Governance Action Group.

### **5.4 Removal of an ACP**

If, during the review process, the Trust RA staff identify that an ACP is no longer required, the RA staff must identify who is currently assigned to the ACP and determine whether the staff in question need to be assigned to a new position.

Once this has been determined, it is necessary to ensure that the change is documented and included within the CIS Position Document and Mapping spreadsheet before it is resubmitted for approval by



the Information Governance Action Group. Upon receiving authorisation, the RA staff will notify the ESR Workforce Management staff member to ensure that the ESR Position Linking is modified in accordance with the change.

If a replacement ACP is not required, the Trust RA staff will notify the staff in question that they will no longer have any NHS CRS Access associated with their Smartcard.

Once these steps have been completed the Trust RA staff will be able to close down the ACP and the ESR Work Structures staff will need to re-run the Submit Request process to remove the ACP from being assigned.

## **5.5 New ACP**

A new ACP can be identified in a variety of ways as follows:

- A new NHS CRS system;
- A request to amend an existing NHS CRS ACP;
- A new ESR Position within the Trust;
- A new NHS CRS ACP;
- Identification through the review process.

When new NHS CRS ACPs are identified the RA staff will need to determine who requires this access and ensure that the CIS Position Document and Mapping spreadsheet is updated before it is submitted to the Information Governance Action Group.

Upon receiving authorisation, the NHS CRS ACP(s) will be created, approved, and granted in CIS before being downloaded into ESR via the Work Structures URP, Submit Request process so that it is available for linking.

## **5.6 ESR Position Linking**

The Trust has identified that, to ensure maximum benefits are achieved; the employed staff will have their NHS CRS Access managed via the ESR-CIS Interface.

The mapping will also need to be considered when creating, amending or removing ESR Positions to ensure that staff assigned to these Positions maintain the correct NHS CRS Access. All Position linking will be completed in accordance with the approved CIS Position Document.

*N.B. The exceptions for this are staff not directly employed by the Trust and who do not therefore have a record on ESR. These staff will be managed via CIS only.*

## **5.7 Amendment to an ESR Position**

The Trust's Workforce Management staff will determine whether the ESR Position in question is/is not linked to an NHS CRS ACP. A review must be undertaken to confirm that either:

- the current NHS CRS ACP is still required;
- a new NHS CRS ACP needs to be approved and created;
- NHS CRS Access no longer required;
- A different existing NHS CRS ACP is required to be linked.

## 5.8 Removal of an ESR Position

Before an ESR position is removed the Trust's ESR staff must check if it is linked to an NHS CRS ACP. If linking is in place the ESR staff must ensure that the staff currently residing in the position are transferred into another position with the relevant NHS CRS Access.

If staff are moved into another ESR Position that does not have an NHS CRS ACP linked the staff will automatically lose their NHS CRS access.

## 5.9 New ESR Position

If a new ESR Position is required, the Trust's Workforce Management staff will ensure that communication is made with the relevant staff within the organisation to ascertain the required NHS CRS access.

## 5.10 Personal Information Management

Now that the ESR-CIS Interface is activated the Trust will use ESR to automatically inform CIS of any personal detail changes, ensuring that the data is kept up to date in CIS and consistent with ESR. Amendments to the data items below, in ESR, will automatically trigger a message to be sent to CIS for 'granting' and RA staff within the Trust will ensure that they regularly monitor CIS to accept/reject these changes.

**Once a message from ESR is granted in CIS, the CIS record is locked and can only be changed via ESR.**

## 5.11 Automated Addition and Revocation of NHS CRS Access

When a Trust member of staff has their assignment status (to an ESR position linked to a NHS CRS ACP) changed from an 'active' status in ESR, a message is sent to CIS via the interface to remove access to NHS CRS applications. This ensures that amendments to NHS CRS access take place in a timely manner, extra resource is not required, and Information Governance is greatly enhanced.

## 5.12 CIS

The Trust acknowledges that there are some instances where staff cannot have their NHS CRS Access managed via the ESR-CIS Interface and these staff will need to have their NHS CRS Access managed via CIS directly.

To reduce potential complications, including training and IT configuration, any requests for new starters, CRS access, modify details and revocation of access through CIS will only be communicated via the IT Portal to RA staff by Line Managers.

## 5.13 External Staff

All new starters in the Trust that fall outside of the ESR-CIS Interface processes, who have no ESR record, will have their Smartcard produced in CIS via the request, approve and grant process.

To reduce training requirements, it has been agreed that the new starter process will be completed within the IT Service Desk Department.

The new starter will attend a face-to-face meeting and produce their ID documentation. The RA Staff will then verify ID and enter the relevant information into CIS and complete the Smartcard process with the new starter

present.

The Trust's IT Service Desk team will assign the NHS CRS Access to the non-ESR staff via CIS using the executive grant approach and a time limit of three months will be set.

#### **5.14 Keep In Touch Days**

Following the relevant member of staff's assignment status changing to "Maternity" in ESR, as required, the Line Manager will, via the IT Portal advise the IT Service Desk Team to request the relevant CRS access be applied.

Upon the member of staff's return, Workforce Management staff will associate the user immediately ahead of their change to an active assignment status.

When the employee returns to work (and the assignment status is changed to 'active') ESR will automatically control NHS CRS access and overwrite any previous access that may have been granted in CIS.

#### **5.15 Non-ESR Staff**

Non-ESR staff NHS CRS Access will only be assigned time limited CRS access. The Line Manager will determine the NHS CRS ACP most appropriate for the user and will advise the IT Service Desk Team via the IT Portal

The Trust's IT Service Desk team will assign the NHS CRS Access to the non-ESR staff via CIS using the executive grant approach and a time limit of three months will be set.

#### **5.16 Change of Access**

Any non-ESR staff requiring a change in NHS CRS Access will notify their Line Manager that their current NHS CRS Access is not suitable for their role.

The Line Manager will then review this request and following consultation with RA staff identify which level of NHS CRS Access is required via email to request an adjustment.

Upon receipt of the request, the IT Service Desk team will revoke the current NHS CRS ACP and assign the relevant NHS CRS ACP via CIS using the executive grant approach with a time limit of three months.

#### **5.17 Leavers**

If the user is moving to another role within the NHS, they should retain their Smartcard and access will be granted by the new NHS organisation.

If the user is not staying within the NHS, the line manager is required to return the Smartcard to the RA Agent within IT Services.

#### **5.18 Non ESR Staff**

The Trust's Workforce Management Staff do not manage the non-ESR staff therefore a separate process is required for removing any NHS CRS Access from those individuals.

In the first instance the IT Service Desk team will introduce a time limit, namely six months or otherwise identified by a specific contract, to this staffing groups' NHS CRS Access. This will ensure that NHS CRS Access will be revoked at the end of the set time period and, if an individual is still in post, NHS CRS Access can then be re-assigned for a further six months.

### **5.19 RA Agent configuration in ESR**

The ESR Supplementary Role of 'NHS CRS RA Agent' is used to record the identity of the RA Agent who performed the identity checks.

The verification of identity forms includes a field 'Enter Name of RA Agent that verified ID' containing a list of all staff members who have been assigned this role.

### **5.20 NACS/ODS Codes in ESR**

The National Administrative Codes Service (NACS) Code is also a crucial element of the ESR-CIS Interface. The Trust has identified one main NACS Code for the organisation (RTG) which is available in ESR and has been added to the Trust level of the hierarchy.

If the NACS Code was to change or a new one added, the Trust's ESR staff must raise a Service Request with the ESR supplier to ensure that the correct NACS Code is made available for use within the Trust Virtual Private Database (VPD). Once this has been completed the NACS Codes must be updated/added in line with the ESR guidance.

As a minimum, the NACS Code must be placed at the Trust level of the organisation's hierarchy and can only be altered or amended by the ESR Work Structures administrator.

### **5.21 RA Notifications in ESR**

RA Notifications are required to be assigned to ESR staff to ensure that messages relating to errors encountered between ESR and CIS are made available on a daily basis.

The Trust has assigned notification roles as appropriate to the staff within Workforce Management that utilise the ESR-CIS Interface and this will be reviewed annually unless any of these staff either leave the organisation or move to another job within the Trust.

The recipients of the notifications within the Trust will ensure that the incoming notifications are checked on a regular basis, at least daily, in order to identify and raise awareness to relevant persons if there are any issues with the ESR-CIS Interface. Workforce Management and RA will review the recipients list every six months to ensure that the notifications are still being sent.

### **5.22 RA URPs in ESR**

The Trust has allocated the required URPs to all relevant staff within the Workforce Management Division whose NHS CRS access contains the requisite RA Agent role. These URPs have been allocated to staff to ensure that multiple people have the ability to carry out tasks within the functionality of the ESR-CIS Interface.

The Trust's Workforce Management staff will review the allocation of these URPs on a regular six-monthly basis, or on an ad-hoc basis if staff/Line Managers identify a need for it, to ensure that they are appropriately assigned to ensure business continuity.

### **5.23 RA Dashboard**

All RA Agents will have access to the Dashboard via the CIS system.

## 5.24 Equipment and Maintenance

The assessment of all resource requirements (Smartcards, printers, printer cartridges) was carried out during the implementation of RA and continues to be reviewed regularly. Printers are serviced as-and-when required. The frequency of servicing printers will be increased to reflect any increase in the issuance of Smartcards. The RA Agents refer to the NHSD website to check for updates to hardware and software on a quarterly basis.

## 5.25 Training

Training on both the ESR and RA systems is provided by Workforce Systems and RA staff and is managed as part of local staff induction. This will maximise the staff's knowledge of the two systems to ensure that they have the ability to use the systems as per the requirements specified by the Trust, ESR and NHSD.

## 6. Monitoring Compliance and Effectiveness

<b>Monitoring Requirement:</b>	Compliance with Information Governance will be monitored against the DSP Toolkit. Assessments are annually to NHS Digital.
<b>Monitoring Method:</b>	The IG Steering Group will monitor compliance with the DSP Toolkit according to the Forward Plan. Where deficiencies are identified, action plans will be developed and these will also be monitored by the IG Steering Group.
<b>Report Prepared by:</b>	Workforce Systems Manager,
<b>Monitoring Report presented to:</b>	Trust Information Governance Group for inclusion in the annual report submitted to the Trust Board through the annual DSP Toolkit report.
<b>Frequency of Report:</b>	Annual report.

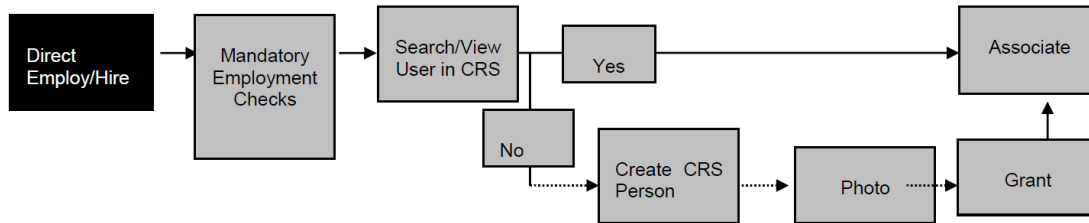
### 6.1 Internal Audit

The issue of Smartcards is subject to an internal audit to ensure that policies are being followed:

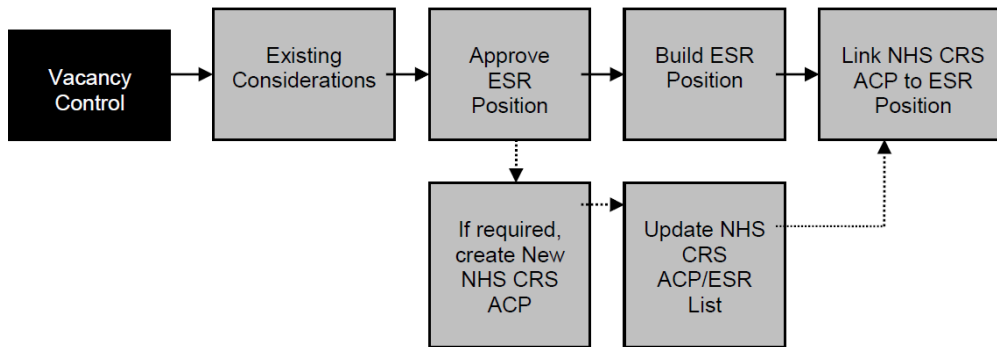
- Applications and records are updated regularly;
- Unused Smartcards are stored safely.

## 1.1 System Processes

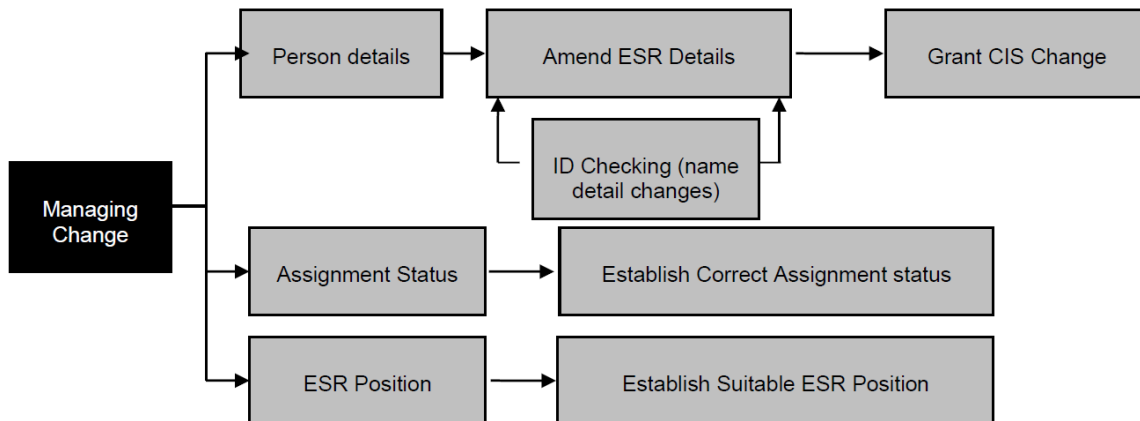
### 1.1.1 New Starter



### 1.1.2 Vacancy Control



### 1.1.3 Managing HR Changes



### 1.1.4 Leavers

