Somerset Partnership NHS
NHS Foundation Trust

LOCAL REGISTRATION AUTHORITY

POLICY AND PROCEDURES

Version:	1
Ratified by:	Senior Managers Operational Group
Date ratified:	July 2015
Title of originator/author:	Clinical Systems Manager - Cerner & Community
Title of responsible committee/group:	Pippa Moger
Date issued:	**July 2015**
Review date:	**June 2018**
Relevant Staff Groups:	All Smartcard Users

This document is available in other formats, including easy read summary versions and other languages upon request. Should you require this please contact the Equality and Diversity Lead on 01278 432000

DOCUMENT CONTROL

Reference	**Version**	**Status**	**Author**
SB/Jul15/LRAP	1	Final	Clinical Systems Manager - Cerner & Community
Amendments	Amended to incorporate recommendations from Caldicott and Information Governance Group		
Document objectives: Guide to the process of maintaining confidentiality of identification information provided for the purpose of registering users or maintaining smartcards and safeguarding patient data.			
Intended recipients: All Smartcard Users and all Registration Authority Managers			
Committee/Group Consulted: Caldicott & Information Governance Group			
Monitoring arrangements and indicators: please refer to section 16			
Training/resource implications: please refer to section 13			
Approving body and date	Caldicott and Information Governance Group	Date: May 2015	
Formal Impact Assessment	Impact Part 1	Date: TBC	
Ratification Body and date	Senior Managers Operational Group	Date: July 2015	
Date of issue	**July 2015**		
Review date	**June 2018**		
Contact for review	Clinical Systems Manager - Cerner & Community		
Lead Director	Director of Finance and Business Development		

CONTRIBUTION LIST Key individuals involved in developing the document

Name	Designation or Group
Stephen Butterfield	Clinical Systems Manager - Cerner & Community
Pippa Moger	Director of Finance and Business Development
Phil Brice	Director of Governance and Corporate Development
Peter Atkinson	Information Governance and Records Manager
Group Members	Caldicott and Information Governance Group
Group Members	Senior Managers Operational Group

CONTENTS

1. INTRODUCTION

1.1 For Healthcare Professionals to access Health & Social Care Information Centre applications they need to be registered. All National Programme applications use a common security and confidentiality approach. This is based upon Role Based Access Control and the healthcare professional's organisation(s), role(s), area(s) of work and business function(s). The primary method that enables trust staff to access National applications is via a Smartcard and Personal Information Number (Passcode) issued during the Registration Process. It is to be noted that we at Somerset Partnership NHS Foundation Trust use Position Based Access Control via the ESR application. The Registration Process is operated at a local Trust level by a Registration Authority that is required to conform to the latest published National Registration Policy and Procedures identified below:

- Registration Authorities Operational Process and Guidance; available from http://systems.hscic.gov.uk/rasmartcards
    - Registration Policy and Practices for Level 3 Authentications Version 3 available from http://systems.hscic.gov.uk/rasmartcards
    - HSCIC Registration Authority Central Policy. http://systems.hscic.gov.uk/rasmartcards/strategy
- Registration Authorities: Governance Arrangements for NHS Organisations.
- the NHS Confidentiality Code of Practice; available from (www.dh.gov.uk)
- NHS Care Records Service Acceptable Use Policy, Terms and Conditions, available from: http://systems.hscic.gov.uk/rasmartcards

1.2 This document describes local Registration Authority procedures necessary to support national policies and procedures to include the management of:

- smartcards for Joiners and Leavers
- smartcards for Locums, Agency and Bank staff
- Personal Information Number/Password maintenance
- role profiles and position based access control
- timely creation and distribution of smartcards
- breaches of security

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

- Registration Authority staff to include Registration Authority Managers, Sponsors and Agents
- Trust Board Members and Senior Trust staff
- Human Resource staff
- Information Technology Services staff
- Confidentiality Specialists including Caldicott Guardians
- Local Health Community Information Technology Support Service or Help desk staff
- Smart Card Users

1.4 This document describes procedures for the operation of the Registration Authority within Somerset Partnership NHS Foundation Trust (hereafter known as the Trust).

1.5 The use of the word staff in this document means individuals who are directly employed by, or contracted to provide service to, or are part of an agreement with the Trust.

2. EXECUTIVE SUMMARY

2.1 Trust staff members that need access to National applications are required to be registered. Once registered, staff will have a Smartcard and Personal Information Number/Password which will allow access to the appropriate applications and information.

2.2 The Registration process is managed by a local Registration Authority. The local Registration Authority is comprised of a Registration Authority Manager, Registration Authority Sponsors and Registration Authority Agents. The Registration Authority Manager (Stephen Butterfield) is appointed by the Trust's Executive Board. Registration Authority Agents and Registration Authority Sponsors are nominated by the Registration Authority Manager.

2.3 The Trust Registration Authority is responsible to ensure that all national and local procedures are followed. These include the registration process, issue and revocation of Smartcards, help-desk support, audit process and the security and confidentiality and data protection policy.

2.4 Registration Authority Managers are responsible to ensure compliance with local and national policies, ensure safe custody, index and retrieval of registration information stored on the local archive, investigate and

report on any cases of abuse or misuse of smartcards, ensure safe storage of Registration Authority toolkits and ensure that periodic compliance audits are performed on the Trust's local Registration Authority process.

2.5 Registration Authority Sponsors are responsible for the identity checks of staff (where applicable), identify staff to Registration Authority Agents and report any abuse or misuse of Smartcards via the Trust's reporting procedure, to the Registration Authority Manager.

2.6 Registration Authority Agents are responsible for the maintenance of smartcards, compliance with national and local policies and adherence to confidentiality rules.

2.7 The Registration Authority process has been integrated with Human Resources policies and procedures with regard to starters and leavers. Starters must be able to meet Registration Authority Level 3 identification requirements and should be registered and trained in the use of Smartcards and applications during the local induction process. Leavers' role profiles and access to National applications are de-activated when the ESR status changes to ex-employee. Staff moving to another NHS location will keep their Smartcard for use in their new organisation. Staff permanently leaving the NHS should return their Smartcard so that it can be destroyed and certificates revoked.

2.8 Lost, Stolen or Broken Smartcards must be reported to the Trust Registration Authority Team as soon as possible. These cards will be revoked and new cards issued by a Registration Authority Agent. Locked Cards and Forgotten Personal Information Numbers should be reported to the local Champion Users as soon as possible.

2.9 Staff members suspecting Smartcard misuse or abuse must report this via the Trust's incident reporting procedure. Depending on the severity of the allegation an investigation may be required. If misuse is discovered appropriate disciplinary procedures must be followed.

2.10 All Registration Authority policies, procedures and processes may be audited by internal or external auditors.

2.11 Agreements may be entered into with other NHS Trusts, Clinical Commissioning Groups and General Practitioner Practices regarding shared services and cross boundary working.

3. SCOPE

3.1 Registration of staff that requires secure authorised access to clinical applications across the Trust includes the following employees:

- substantive (fixed term)
- contract
- locum staff
- agency staff
- bank staff

3.2 Resources in scope include:

- Registration Authority agents to maintain smartcards across the Trust
- smartcard Readers
- smartcards
- local Archive
- accommodation with one network point and one electrical point minimum
- Registration Authority Toolkits (Including Card Printers)
- RA01, RA02 and RA03 forms
- double-sided badge and smartcard holders
- identity Agent Software

4. TRUST REGISTRATION AUTHORITY

4.1 The Registration Authority is an official within the Trust with appropriate organisational authority that is responsible to ensure that all aspects of registration services and operations are performed in accordance with National Policies and procedures. They are responsible for providing arrangements that will ensure tight control over the creation, maintenance and revocation of Smartcards, whilst providing efficient and responsive service that meets the needs of Trust staff.

4.2 Initially, executive management team identified and appointed candidates to perform the Registration Authority Manager and Sponsor roles. The Trust appoints a Lead Registration Authority Manager who subsequently nominates Sponsors and Registration Authority Agents. The Registration

Authority Team registers staff, devices and computer applications within their locality.

Registration Authority Structure

4.3 Each Registration Authority delegates authority to the organisation beneath it. The Registration Authority comprises of Registration Authority Managers, Sponsors and Registration Authority Agents (includes at least one Human Resources Department representative) with authority delegated by a Superior Registration Authority to register Trust users.

4.4 The Registration Authority Reporting structure is as follows:

Nominated Director:
Registration Authority Manager:
Assistant to Registration Authority Manager:
Nominated Sponsors:
Registration Authority Agents:

Please refer to Appendix A.

Trust Registration Authority Responsibilities

4.5 The Trust Registration Authority has the following responsibilities to ensure:

- Registration Authority members are familiar with, understand and adhere to in full Registration Policy and Practices for Level 3 Authentication, Registration Authorities Operational Process and Guidance and this document
- the registration information (RA01) and revocation (RA03) forms are appropriately used. RA03 forms rarely used as HR forms supersede.
- any local processes developed to support the National Registration processes are adhered to in full
- there is sufficient availability of resource to operate the registration processes in a timely and efficient manner to meet their organisational responsibilities
- Registration Authority team members are adequately trained and familiar with the local and national Registration Authority processes
- an alphabetical folder and secure audit trail is maintained of the applicants' Registration Authority forms
- All completed application forms and associated documents are kept secure in an area where the Registration Authority team have access, in line with HSC 1999/053 which stipulates the retention duration for

records. Note Registration Authority records need to be kept for 6 years on leaving the NHS or 70th birthday, whichever is soonest.

- Sponsors are familiar with and understand User Registration – Sponsor Briefing available from http://systems.hscic.gov.uk/rasmartcards
- Notification of the creation and revocation of Registration Authority managers (including their e-mail address and contact phone number) by sending an e-mail to ramanagers.agents@nhs.net

- There are sufficient Smartcards and Smartcard issuing and maintenance equipment (Registration Authority Toolkits) for the organisation. Refer to Registration Authority Hardware Ordering Process. Note: see Registration Authority Hardware Ordering Process and Registration Authority Hardware Ordering Process

- http://systems.hscic.gov.uk/rasmartcards

- Registration Authority sponsors identified via the Executive have the business function of 'Sponsors' associated with the appropriate organisation job profile/s

- Registration Authority Managers identified via the Executive have the business function of Registration Authority Managers associated with the appropriate organisation job profile/s

4.6 All Trust Registration Authority Members have sufficient training to carry out their Registration Authority tasks in accordance with National Policies and Procedures. Registration Authority Team members are individuals capable of trust as they will handle sensitive information covered by The Data Protection Act. Registration Authority Team members are responsible for Trust compliance with the NHS Code of Confidentiality and NHS Care Records Service Acceptable Use Policy, Terms and Conditions.

Trust Registration Authority Managers

4.7 Registration Authority Managers are initially nominated by a Trust Executive and are responsible for establishing day to day operations of the Trust Registration Authority service. Registration Authority Managers ensure that all Registration Authority procedures are carried out in accordance with local and national policies.

4.8 A Trust Executive can nominate a Lead Registration Authority Manager who is then authorised to nominate Registration Authority Sponsors and/or Registration Authority Agents.

4.9 All Registration Authority Managers are required, regardless of length of employment, to provide documentary evidence to prove their identity.

Registration Authority Managers Responsibilities

4.10 Trust Registration Authority Managers have the following responsibilities:

- lead Registration Authority Manager - Manages local Registration Authority and Subordinate Registration Authority Managers, ensures local joiner/leaver amendments are completed.
- lead Registration Authority Managers - Nominate for approval by the trust, individuals who will act as Registration Authority Agents and Sponsors
- review, approve and adhere to trust policies and procedures where applicable, to comply with the national requirements as laid down in the national policy
- ensure safe custody, index and retrieval of registration information held on RMS database
- investigate and report on any cases of abuse or misuse of cards to the superior Registration Authority
- ensure Registration Authority Toolkits and Smartcards are stored in a secure location
- register any Subordinate Registration Authorities within their Trust, including verifying subordinate Registration Authority Agent identification and authorisation
- maintain the confidentiality of identification information provided for the purpose of registering Subordinate Registration Authorities
- ensure that annual compliance audits are performed on the subordinate Registration Authorities and Registration Authority processes in the trust
- become conversant with Setup and Operation, Level 3 Authentication Policy and Registration Authority Operational Process and Guidance documents
- maintain the confidentiality of identification information provided for the purpose of registering users or maintaining smartcards

Registration Authority Manager Appointment

4.11 The executive board will identify a Lead Registration Authority Manager. Subsequent Registration Authority Managers will be nominated by the Lead Registration Authority Manager and formally notified to the Trust Board and the Superior Registration Authority Manager. All Registration Authority Managers' names and User's Unique Identifier will be emailed to the national team (ramanagers.agents@nhs.net)

Registration Authority Manager Reporting

4.12 Registration Authority Managers will report significant incidents to the Trust Board as per the Trust's Incident Reporting Procedure.

Registration Authority Sponsors

4.13 The Registration Authority Sponsor is a designated individual who will identify staff members, staff profiles and the position staff will be employed in to assist Position Based Access Control required for each National application, for example: General Practitioner, Practice Manager, Clinic Manager, or Consultant, to a Registration Authority Agent or Registration Authority Manager.

4.14 Sponsors cannot be self-appointed, they cannot delegate their responsibilities, nor can they sponsor other sponsors. Sponsors must be registered in the Personal Information Number User Directory (Personal Information Number User Directory) before they can sign Registration Authority forms and/or vouch for staff's identity.

4.15 All Registration Authority Sponsors are required to provide, regardless of length of employment, documentary evidence to prove their identity and be registered in the Personal Information Number User Directory before Sponsors can sign RA01 and RA02 Forms.

- Registration Authority Sponsors should be aware and familiar with User Registration - Sponsor Briefing:

  http://systems.hscic.gov.uk/rasmartcards

  and the briefing material relating to the applications for which they will be sponsoring access. Registration Authority Sponsors should also be aware and familiar with Registration Policy and Practices for Level 3 Authentications and Registration Authority Operational Process and Guidance documents

  http://systems.hscic.gov.uk/rasmartcards

Registration Authority Sponsor Responsibilities

4.16 Registration Authority Sponsors have the following responsibilities:

- Identify the organisation they belong to and their Role Profile

- attendance at the face to face meeting to confirm the identity of the user. Note: Sponsors should not view identification documentation; validation of documentation is an agent role

- read and sign the User Registration form (RA01 Part A and part B) acknowledging that he/she understands and agrees to the obligations

described therein

- complete and sign User Profile Additions and Modification form (RA02) for users whose roles are changing

- complete and sign Request to Cancel Smartcard or form (RA03)

- sponsors will also register for digital certificates for fall back authentication smart cards. Fall back authentication smart cards are to be used by users over which the Sponsor has management responsibility in instances where staff cannot use their own smart card for authentication to NHS systems; such as: card forgotten, lost/damaged (but replacement not yet issued).

4.17 Maintain the confidentiality of identification information provided for the purpose of registering users or maintaining smartcards.

4.18 Registration sponsors are responsible for ensuring that National Program application users are given the minimum appropriate level of access required needed to do their job. The areas of responsibility with respect to National Program application user access should be clearly defined for each sponsor.

Registration Authority Sponsor Appointment

4.19 Sponsors are identified, appointed and entrusted to act on behalf of the Trust Executive team or Caldicott Guardian as being suitable persons, by virtue of their status and role, in determining who should have what access and maintaining the appropriateness of that access.

4.20 Registration Authority Sponsors will be the operational heads, clinical managers, line managers or administrators within a practice, clinic or department using a National Application.

4.21 Authorised Sponsors are registered by a Registration Authority Manager or Registration Authority Agent on behalf of the Trust Executive with instructions given by the Trust Executive or by the Trust Lead Registration Authority Manager.

Registration Authority Sponsor Reporting

4.22 Registration Sponsors are required to report any Registration Authority related incidents, using the Trust incident reporting procedure to the Registration Authority Manager. Additionally, Sponsors will report any operational difficulties especially where these have patient healthcare implications to the Registration Authority Manager and the Caldicott Guardian.

Registration Authority Agents

4.23 Registration Authority Agents are responsible to the Registration Authority Manager for ensuring that National and local processes are followed. Registration Authority Agents will ensure that all inter Trust agreements are followed and adhered to. All incidents, misuses, anomalies and problems will be reported to the Registration Authority Manager. All Registration Authority Agents will be suitably trained.

4.24 Registration Authority Agents are specifically responsible for the following:

- issuance of Smartcards and all cryptographic keys contained on the card
- familiar and compliant with all national and local policies/procedures
- compliance with national and local policies and procedures
- adherence to strict confidentiality rules
- note: Sponsors should not view identity documentation; validation of documentation is an Agent role

4.25 Registration Authority Agents will only register users within the Trust unless there is a formal agreement with another NHS organisation. In such cases the Agents will comply in full with the inter-trust agreement(s), which must be compliant with national policies and procedures.

4.26 Registration Authority Agents will only action requests from a recognised Sponsor, Registration Authority Manager or the Trust Executive, which comply with the National and local policy and procedures.

4.27 All Registration Authority Agents are required, regardless of length of employment, to provide documentary evidence to prove their identity.

5. HUMAN RESOURCES PROCESSES

5.1 The Trust will ensure that the process supporting the identification, registration and management of staff will be integrated with other Trust processes, as appropriate. The following Trust policies integrate with the Registration Authority process and therefore will be amended to reflect Registration Authority policy and procedures:

- recruitment process
- joiners and Leavers
- agency, locum and bank staff
- non-NHS staff/Contractors (social workers and counsellors)

- disciplinary process

Process Flowcharts

5.2 The pre and post-employment flowchart is the responsibility of the RA Manager and can be found in Appendix B.

Recruitment

5.3 When all staff are recruited the following points must be considered:

- checks on an applicant's identity are made during the recruitment process to ensure Registration Authority Level 3 identification requirements are met. Identification requirements are detailed in Registration Policy and Practices for Level 3 Authentication

- notification of new employees' start date and department are sent to Trust Registration Authority Managers, and Agents

Starters

5.4 As part of local induction process for new staff that requires access to use National Applications, the responsibility lies with Line Managers and the following points should be considered:

- relevant Sponsor to identify the appropriate role profile and level of access to each application and complete a RA01 form

- **if a staff member already holds a Smartcard issued by another Trust**, authorising the necessary Role Profile/s and completing an RA02 form

- introduce new starters to the Registration Authority registration process

- ensure staff acknowledge they have read and understood Registration Authority Policies and Procedures governing the use of Smartcards and National Applications by reading and signing Part A and part B of the RA01 form

- ensure a training needs assessment and training is completed based on the role profile(s)

5.5 Where full registration is required; the Applicant will be required to present suitable forms of identification in accordance with Registration Policy and Practices for Level 3 Authentication (if it was not presented to Human Resources during the recruitment processes).

5.6 All the above tasks will be integrated into the standard Trust employment processes, as much as possible to prevent duplication.

Use of Name

5.7 The name to be used for Registration Process needs to be the name the individual has used for their employment in the organisation such as their employment name. Where this differs due to marriage/divorce/deed poll, from the documentary evidence provided proof, through the appropriate marriage/divorce/deed poll certificate is required. It is not necessary that all identity documentation shows a consistent name in these circumstances only.

5.8 Should the user desire a different familiar name to be printed on the Smartcard then the Registration Authority needs to be assured that this name is the familiar name by which the individual is known. In these cases the Registration Authority is required to update Part 1 of the RA01 to record both the employment name and familiar name and to get the user to initial these changes. T he principle here is that the name on the Smartcard need not be the employment name, provided the name change is reasonable, established and documented on the RA01 (as determined by the Registration Authority Agent, Registration Authority Manager or Trust Executive).

Leavers

5.9 During the leaving process the Line Manager will establish, with the Registration Authority Sponsor or Leaver, whether the staff member is leaving the NHS permanently or joining another NHS organisation and inform the RA Manager accordingly.

5.10 When staff leave, the following points must be considered:

- all Trust role profiles in the Personal Information Number User Directory pertaining to the employee will be deactivated when the ESR status changes to ex-employee.

- if the User is transferring to another NHS related location such as. General Practitioner practice, Primary Care Trust and they can provide details/proof then the current registration details will be copied and sent to the new location, the user is allowed to retain the Smartcard but their Trust profile in this organisation is deactivated

- staff permanently leaving the NHS should have the certificate revoked and their Smartcard destroyed

- staff on long term leave should have system access revoked and the Smartcard should be securely stored with the Line Manager or Trust Registration Authority. In cases of changes to ESR to reflect long term absence e.g. maternity leave the card link is de-activated.

- records must be kept of all cards that have been returned and destroyed. If returned cards are not destroyed immediately, they must be kept in a secure environment until such time as they are destroyed

- the Registration Authority Manager and Registration Authority Agent must be notified via email giving as much notice as possible

- the required actions must be taken on the last day of employment after the staff member leaves the Trust

Agency, Locum and Bank Staff

5.11 When temporary staffs need access to National applications as part of their role, the following points should be considered:

- staff working as part of a team may not need a Smartcard to carry out their role

- some temporary staff could already be enrolled in the Personal Information Number User Directory and will only require role profiles changed or added

- temporary staff who are Smartcard holders may not have sufficient training in the use of a particular National Application, so a training needs assessment will be required

- contact agencies to facilitate pre-registration of staff

- create cards without role profiles. Role profiles to be added when staff presents at work and upon completion of a RA02 form

Non-NHS Staff/Contractors

5.12 The Trust will ensure all contractors who need to use the National applications are bound to the Data Protection Act and The NHS Confidentiality Code of Practice (www.dh.gov.uk). This will include the process to be taken in cases of a breach of security and liability issues.

6. SMARTCARD MANAGEMENT AND USE OF REGISTRATION AUTHORITY EQUIPMENT

6.1 The Registration Authority Manager, on behalf of the Trust, is responsible for ensuring that adequate numbers of Smartcards are available and maintained throughout their useful life.

6.2 The Information Technology Manager will ensure that there is sufficient computer equipment to support all users of National applications (including those for registration).

6.3 The Registration Authority Manager will ensure that there are appropriate numbers of toolkits available for Registration Authority use, that the toolkits are kept in a secure environment and that they are used and maintained appropriately.

6.4 All Registration Authority equipment will be subject to policies and procedures governing the management and control of Trust Assets.

Smartcard Management

6.5 Issuing smartcards can only commence if the Registration of staff is completed successfully.

6.6 The process for smartcard issuance is generally by post, with the passcode emailed separately, or by face to face with the Registration Authority Agent/Registration Authority Manager.

User/applicant presents:

- one personal identity document (current Passport or European Union Photo Drivers License) and
- two active in the community documents (local authority tax bill, bank statement, utility bill (less than 3 months old), local council rent card, tenancy agreement, benefit book, mortgage statement.)
- note: Mobile Phone bills are <u>not</u> acceptable as an active in the community document

  OR

- two personal identity documents and
- one active in the community document
- note: A list of acceptable identifying and active in the community documents can be found in Registration Policy and practices for level 3 Authentications document v3 and Registration Authority Operational Process and Guidance document
- the Registration Authority Agent verifies the user/applicant's information and photograph, authenticates the Applicant's identity documents and records the identification information on the RA01 form (Sponsors should not view identity documentation)
- the Registration Authority informs the user of his/her responsibilities; i.e. the need to protect the Personal Information Number (Passcodes)

Identity Management Guidelines

- identity assurance is increasingly important for the NHS, both for recruitment and for access to the NHS Care Record Service. The Department of Health 'NHS Employment Check Standards' published by NHS Employers include the checks that are required by law, those that are Department of Health Policy, and those that are required for access to the NHS Care Record Service

- the six standards replace the previous NHS Employers guidance on safer recruitment and outline the employment checks NHS organisations must perform to meet the Department of Health's core standards, measured in the Healthcare Commission's annual health check

- all six documents can be found at: http://www.nhsemployers.org/primary/Employment-checks.cfm

- per National Policy, all Registration Authority Managers, Sponsors and Agents must provide a minimum of three forms of identification, as per Section 6.1, regardless of the number of years they have worked for the Trust

Verification of Identity

6.7 Verification of identity checks are designed to:

- determine that the identity is genuine and relates to a real person

- establish that the individual owns and is rightfully using that identity

6.8 The NHS uses two methods for verifying identity: requesting original documents and checking an individual's personal details against external databases.

6.9 Original documents allow you to check an employee's:

- full name – forenames and last name

- signature

- date of birth

- full permanent address

6.10 Prospective employees must provide acceptable documents containing their photograph, such as a passport or United Kingdom driving licence, and acceptable documents providing their current address. A face-to-face meeting is also an essential part of the verification process.

6.11 Employers must record the outcome of the checks using Electronic Staff Record (ESR), confirming that identity has been verified in accordance with these standards.

Acceptable Personal Identification Documents

6.12 Some documents are more reliable than others and only certain documents, in certain combinations, are acceptable for verification of identity.

6.13 Prospective employees will need to provide either of these two combinations:

- two forms of photographic personal identification and one document confirming their address
- one form of photographic personal identification and two documents confirming their address

6.14 All documents must be originals, or copies of originals certified by a solicitor.

6.15 Where a signature has not previously been provided, for example because of an e-application, the individual should be asked to provide it at interview for checking against relevant documentation.

Acceptable Photographic Personal Identification Includes:

- current United Kingdom (Channel Islands, Isle of Man or Irish) passport or European Union/other nationalities passport
- passports of non-European Union Nationals, containing United Kingdom stamps, a visa or a United Kingdom residence permit showing the immigration status of the holder in the United Kingdom*
- a current United Kingdom (or European Union/other nationalities) photo-card driving licence (providing that the person checking is confident that non-United Kingdom photo-card driving licences are bona fide)
- a national identification card and/or other valid documentation relating to immigration status and permission to work*

6.17 Any document that is not listed above (such as an organisational identification card) is not acceptable.

6.18 For further information on immigration please refer to the Right to work checks document of the 'NHS Employment Check Standards'.

What if No Acceptable Photographic Documentation is Available?

6.19 If an individual seems genuinely unable to provide any acceptable photographic personal identification, then two forms of non-photographic personal identification, and two documents confirming their address must be provided. All four documents must be from a different source.

6.20 In addition, they will need to provide a passport-sized photograph of themselves, endorsed on the back with the signature of a 'person of standing' in their community who has known them for at least Human Resources three years. A 'person of standing' could be a magistrate,

medical practitioner, officer of the armed forces, teacher, lecturer, lawyer, bank manager or civil servant.

6.21 The photograph should be accompanied by a signed statement from that person, indicating the period of time that the individual has been known to them. Always check that the signature on the statement matches with the one on the back of the photograph and that it contains a legible name, address and telephone number. A copy should be taken and retained on file. All copies should be signed, dated and certified by the person taking the copy. It is good practice to contact the signatory to authenticate the details of the statement.

Acceptable Confirmation of Address Documents Include:

- recent utility bill (gas, electricity or phone) or a certificate from a supplier of utilities confirming the arrangement to pay for the services on pre-payment terms (note: mobile telephone bills should not be accepted as they can be sent to different addresses). Utility bills in joint names are permissible*
- local authority tax bill valid for the current year*
- current United Kingdom photo-card or old-style driving licence (if not already presented as a personal identification document)
- bank, building society or credit union statement or passbook containing current address
- most recent mortgage statement from a recognised lender*
- current local council rent card or tenancy agreement*
- current benefit book or card or original notification letter from Department of Work and Pensions (DWP) confirming the rights to benefit
- confirmation from an electoral register search that a person of that name lives at the claimed address*
- court order

6.22 The date on these documents should be within the last six months (unless there is a good reason for it not to be, such as clear evidence that the person was not living in the United Kingdom for six months or more) and they must contain the name and address of the applicant.

6.23 Acceptable non-photographic proof of personal identification documents include:

- full United Kingdom birth certificate – issued within six weeks of birth

- current full driving licence (old version) – provisional driving licences are not acceptable
- residence permit issued by the Home Office to European Union Nationals on inspection of own-country passport
- adoption certificate
- marriage/civil partnership certificate
- divorce or annulment papers
- police registration document
- certificate of employment in HM Forces
- current benefit book or card; or original notification letter from the Department of Work and Pensions confirming legal right to benefit
- most recent tax notification from HM Revenue and Customs (formerly Inland Revenue)
- current firearms certificate
- application Registration Card issued to people seeking asylum in the United Kingdom (or previously issued standard acknowledgement letters, SAL1 or SAL2 forms)
- GV3 form issued to people who want to travel in the United Kingdom 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 (formerly Inland Revenue)

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

- full United Kingdom birth certificate – issued within six weeks of birth
- national Insurance number card or proof of issue of a National Insurance number (this will also be a Human Resources requirement for employment)
- certificate of educational qualifications (certificates should be originals from the school/university/awarding body)

Fallback Cards

6.25 Sponsors can register for digital certificates for fall back authentication smart cards. Fall back authentication smart cards are to be used by users over which the Sponsor has management responsibility in instances where staff cannot use their own smart card for authentication to NHS systems; such as card forgotten, lost/damaged (but replacement not yet issued). This is covered in more detail in the Registration Authority Operational Process and Guidance document.

Lost, Stolen and Broken Smartcards

6.26 Lost and damaged Smartcards should be reported to the Registration Authority Team as soon as is practicable. Once notified that a Smartcard has been lost or damaged, Registration Authority Agents will arrange to have the lost/damaged Smartcard revoked and replaced as soon as possible. In the case of loss or theft the Registration Authority Manager must be informed so that checks may be made to ensure that the Smartcard has not been misused. A Datix form is required to authorise replacement of these cards.

6.27 When an issued Smartcard becomes unusable or it is lost or stolen the Smartcard certificate must be revoked. Revocation renders the Smartcard useless.

6.28 As long as the Smartcard holder's identity can be verified at a face to face meeting a new Smartcard may be issued by the Registration Authority Agent.

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

Personal Information Number/Passcode Unlocking and Changing

6.30 Users who have forgotten their Personal Information Number/Passcode or suspect that it may be known by another or who have been locked out of National Applications because of Human three failed login attempts; should report the problem to the Registration Authority Team as soon as is practicable.

6.31 Once notified the Registration Authority Agents/Sponsor will arrange to have the Personal Information Number/Passcode reset/changed with the user. The Smartcard holder and Smartcard must be present unless using the Remote Password Reset process.

Misuse/Revocation

6.32 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

6.33 Revocation tasks can only be carried out by Registration Authority Managers. Where the revocation is needed due to a staff member leaving the NHS, Human Resources will inform the Registration Authority Manager accordingly so that the correct actions can be taken (Personal Information Number User Directory/Card Management Service).

6.34 Where the revocation has been requested by Line Managers because of security related events, the Registration Authority Manager will authorise the appropriate action and inform the following staff as appropriate:

- Registration Authority Agent
- Human Resources Manager
- relevant Sponsor(s)
- Registration Authority User
- Caldicott Guardian

6.35 Revocation renders the Smartcard useless.

Expired Certificates

6.36 Smartcards are valid for four years; certificates are valid for two years. Once the certificate has expired, the smartcard will not log on to the NHS Personal Information Number. Prior to their expiration date, the Registration Authority Agent should arrange with the user to renew the certificates. It would be advisable for the Registration Authority Team to keep a record of the date of issue of each smartcard, so that a schedule of renewals can be produced, pending the release of the Identity Agent software version 11 which will inform the card holder of the expiry date at log in and allow self-renewal of the certificates. A self-renewal process is currently in production.

Toolkit Management

6.37 The full Registration Authority toolkit comprises of a laptop computer, smartcard printer, card reader, hub and associated mains, network and USB cables. Toolkits should be treated with care, used appropriately and protected to prevent loss or damage. The Registration Authority Agent and Registration Authority Manager are responsible for toolkits and their secure storage.

7. REGISTRATION

Registration Authority Forms

7.1 The Trust may add to the Registration Authority forms published nationally provided they do not remove any of the original content or dilute it in any sense and ensure that all subsequent changes to the national forms are incorporated within two weeks of their notification.

7.2 The Trust will ensure they use the latest version of the Registration Authority forms as published on the website http://systems.hscic.gov.uk/rasmartcards and ensure it is up to date with the National forms.

7.3 Trust Registration Authority Team members will receive Training on the Registration Authority forms and their use. Special training will be arranged whenever Registration Authority forms are changed significantly.

7.4 All forms should be completed correctly and completely prior to the issuing of any new card or change of role.

7.5 Completed forms must be kept locked in a secure cabinet until they can be handed to personnel, where they are placed in the applicant's personnel file. These forms are to be kept in accordance with National policy on record retention.

7.6 It is important that any unused boxes on these forms are struck through so no additions can be made to the Sponsors request/s.

Registration Authority 01 (RA01) – New Registration

7.7 The RA01 form is used to record the registration of new National Application Users and should be used as published on the website: http://systems.hscic.gov.uk/rasmartcards

7.8 The RA01 is in three sections:

- section 1 Applicant details: To be completed and signed by the applicant
- section 2 Glossary of Terms
- section 3 Sponsor Declaration: To be completed by the Sponsor (conformant to the Registration Policy and Practices for Level 3 Authentications).For Registration Authority and Sponsor use only

7.9 The RA01 form is held by the applicant until the Registration Authority Manager/Agent registers the applicant on the NHS Spine User Database. Once registration is completed the RA01 form is delivered securely to the Human Resources department or Line Manager where the Registration

Authority forms are logged and filed, are to be available for Registration Authority Managers/Agents/Sponsors/auditors as necessary. Registration Authority forms should be transported in sealed opaque envelopes.

7.10 The RA01 form is used by the Sponsor to convey the need for a Smartcard to the local Registration Authority. Sponsors need to complete Part 2 of the RA01 form.

Registration Authority 02 (RA02) – Profile Changes

7.11 The RA02 form is used to record changes made to an existing National Application User's Role Profile(s). This will be necessary whenever an employee starts, moves departments or job role or ends employment with the Trust.

7.12 Whenever a change to a User's Role Profile is identified the relevant Sponsor must be requested to authorise the changes required. The following are examples of when Role Profile changes would be needed:

- a Medical Admissions Secretary changes departments
- a Senior Nurse covers a colleague's role as a Nursing Manager during a period of sick leave or holiday
- an Administrator takes on an extra job in a different department
- a General Practitioner Registrar's assignment in a General Practitioner Practice comes to end

7.13 Changes of access occur when the employee position is changed on ESR. This is actioned on receipt of a changes form.

Registration Authority 03 (RA03) – Revocation

7.14 The RA03 is used to record revocations. Whenever it is necessary to revoke a certificate associated with a Smartcard a RA03 form must completed and signed by the Sponsor. Sponsor should only do this when it has been confirmed by Human Resources the user has left the organisation or in the case of disciplinary action, on the express request by Human Resources. Once complete the RA03 should be sent to the Registration Authority team for action. This is rarely used in organisations linked to ESR.

7.15 The Registration Authority team need to cross check revocations with Human Resources prior to making any changes to ensure they revoke the access of the correct user and be especially diligent.

7.16 The smartcards should be retained by the Trust and then destroyed as soon as is practical after the staff member has finished.

7.17 The RA03 form is used by the Sponsor to revoke someone's access to all National Programme applications for an Organisation. Sponsors need to complete the whole of the RA03 form. It is anticipated that the main usage of this form will be when a user loses a Smartcard, leaves the Health Service, a Smartcard ceases to work, or is instructed by the Human Resource function and/or Caldicott Guardian to revoke a user's access to National Programme Applications for an Organisation.

Profiles

7.18 What a user is able to access is based on the information in the profile. Whenever there is a temporary and permanent change in the way a person works, a review of the person's National Program application access must be carried out. If there are significant changes to the staff member's role the relevant Role Profile on the Personal Information Number User Directory must be requested via a suitable Sponsor.

7.19 Examples of changes that would necessitate profile changes are as follows:

- job Title
- access requirements
- department
- site(s)
- work Group
- organisation

7.20 It is recommended for changes to profiles that a changes form is completed as within the PBAC process this automatically happens on receipt.

- sponsors name and their Smartcard Unique User identification number
- user's name and Smartcard number
- new role/function as described in the National Programme application or in the local organisation
- removal of profiles which are no longer appropriate to the Healthcare Professional
- completed request are sent via a paper copy or by a digitally signed Email to the Registration Authority

7.21 New roles should be added to the Personal Information Number User Directory entry prior to the start of the new role so that the profile is available for use.

Operating a Bureau Style Model

7.22 To operate a bureau style service, a Registration Authority must use the following process:

- the organisation has delivered the governance framework information and an explanation of the Registration Authority process, including support, escalation arrangements, local sponsor contacts, helpdesk procedures
- users complete an RA01 form, requiring a sponsor's signature
- where necessary, sponsor signs a completed profile assignment RA02 form
- either an Registration Authority Manager or Registration Authority Agent attends the applicant's site
- Registration Authority manager or agent arranges a face-to-face meeting with the user, checks the user's credentials, refer to section 3.1.3:
  Acceptable Personal Identification Documents', and that RA01 (and RA02) forms are complete
- Registration Authority manager or Agent takes a photograph of each applicant, ensuring that each photograph is associated with the correct RA01
- at the applicant's site, or a site with Smartcard printing capability, Registration Authority Manager or Agent registers the applicant in the NHS Spine User Directory leaving the Account Recovery Passcode and Verification Passcode fields blank for the applicant to enter when issued with their Smartcard
- Registration Authority manager or Agent imports the user from the Personal Information Number User Directory into the Card Management System (Card Management Service), and creates and prints a Smartcard using random Smartcard logon Passcodes that are not recorded
- at the applicant's site, the Registration Authority Manager or Agent issues the Smartcard to the user, using the photograph on the Smartcard and user's name as proof of identity. When issuing the Smartcard the Registration Authority manager or agent asks the user to reset their Smartcard Passcode, and enter an Account Recovery Passcode and Verification Passcode where required via the Self Service Portal. Smartcards must not be given to users unless this is

done. For more information about the Self Service Portal, refer to the Registration Authority Operational Process and Guidance document

- the applicant signs a statement confirming they have changed their Passcodes to ones only known to them. Organisations should modify the RA01 to include 'By signing this document, I, the applicant, confirm the Passcode has been reset to one only known to myself'

- a different Registration Authority Manager or agent verifies the signatures against the RA01 user signatures, and ensures there are signatures for all Smartcards issued. If signatures do not match, the Registration Authority should revoke the access associated with the Smartcard, investigate and take remedial action

- Registration Authority forms are stored according to the organisation Registration Authority policy together with proof of Passcode change confirmation

7.23 Any unclaimed Smartcards, for example when a user becomes ill and cannot collect their Smartcard, should be stored with the Registration Authority forms. If the Smartcard cannot be issued to the user, the Smartcard should be cancelled in the Card Management Service, the NHS Spine User Directory person record deleted, and the Smartcard physically destroyed.

Confidentiality of Information

7.24 All personal data held by the Registration Authority relating to the registration processes (such as RA01, RA02) are considered to be sensitive information and must be protected in accordance with the Data Protection Act (1998). It is recommended that all Registration Authority forms are stored by the Registration Authority Manager and Agents. These are accessible on request.

Protection measures are as follows:

- storage must be locked, secure, and limited in access to those individuals in the Registration Authority network who are actively processing registration information

- registration Authorities are bound by the requirement to maintain the confidentiality of personal information provided to them as part of the authentication process

- registration Authorities should only log details of the users personal identity evidence that has been used on the RA01 (Passport, Driving Licence and Birth Certificate numbers)

- registration Authority Agents should record only the name of the originating organisation of any supporting Active in the Community documents[1]

- sponsors are not required to have sight of any personal identity documents relating to Certificate Applicants

Archive Requirements

7.25 The retention of evidentiary information used for authentications must be fully compliant with requirements. The following text is reproduced for the retention requirements of Establishment Records – Major, a category that includes personnel files:

- keep for six years after subject of file leaves service, or until subject's 70th birthday, whichever is the later. Only the summary needs to be kept to age 70; remainder of file can be destroyed six years after subject leaves service

7.26 The following guidance contained is also applicable to the retention of identification information for NHS level 3 authentications:

- where practical, file copies of the supporting evidence should be retained. Alternatively, the reference numbers and other relevant details of the identification evidence obtained should be recorded to enable the documents to be obtained again. Where checks are made electronically, a record of the actual information obtained, or a record of where it can be obtained should be kept

8. INCIDENT REPORTING

8.1 Incidents may be reported by any member of staff (in accordance with the Trust's Untoward Events Reporting Policy and Procedure) where they feel that there is a risk to patient health, confidentiality or Trust reputation. Incidents should be reported to the Registration Authority Manager using the Trust Incident Procedure.

8.2 Examples of incidents are:

- smartcard or application misuse

- smartcard theft

- non-compliance of Local or National Registration Authority Policy

- any unauthorised access of National Applications

- any unauthorised alteration of patient data

[1] National documentation requires that all numbers are recorded. However, due to identity theft concerns, the Trust will only record the name of the originating organisation of the document.

8.3 The Registration Authority manager will consider all incidents reported to them. Any incidents considered significant will be escalated to the Trust Board, Human Resources and/or the Trust Caldicott Guardian depending on the nature of the incident. A major breach of security will also be reported by the Registration Authority Manager to the Local Service Provider, Cluster and Superior Registration Authority Manager (Strategic Health Authority Registration Authority Manager) to ensure any risks resulting from the event can be taken into account and mitigated against.

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

8.5 Incidents involving breaches of security or smartcard misuse demonstrate that a User may not be considered trustworthy. All incidents of this type should be reported to the Registration Authority Manager so that appropriate measures may be taken. In discussion with Human Resources it will be decided which other members of staff need to be involved (such as line manager, Information Technology Manager, Caldicott Guardian).

8.6 In cases of serious misuse or abuse, the Registration Authority Manager in consultation with Human Resources, the Caldicott Guardian and any other member of staff considered appropriate by Human Resources, should revoke the user's certificates pending an investigation and in accordance with the Trust's disciplinary procedures. In the event that an investigation clears the user of any wrong doing, the certificates can be re-issued. If the investigation confirms the suspected abuse, the Trust's disciplinary procedures should be followed.

9. BREACHES OF SECURITY

9.1 Breaches of Smartcard Security will be investigated in accordance with the Trust Disciplinary Policy and may result in disciplinary action.

10. LOCAL REGISTRATION AUTHORITY SUPPORT

10.1 To ensure Trust staff are appropriately and efficiently supported, the following points need to be considered:

- 24 hour support should be provided where necessary when to do otherwise would compromise patient care and confidentiality
- a specific team may be appointed whose sole responsibility is to provide Registration Authority support to users
- existing personnel in various departments (Human Resources, Information Technology, Training, Medical Records) may be appointed to act as Registration Authority Agents and Sponsors in addition to their normal roles

- it would be helpful for users to have a single point of contact for Registration Authority support issues

- additional training for support staff on likely card issues would be an effective way of managing problems, allied with a number of simple scripts to try and isolate the nature of the problem and re-direct the card holder to the appropriate resource to assist them

10.2 Registration Authority support will be carried out jointly by the Trust and TST Registration Authority as follows:

- key resources across the Trust operations, supplemented by TST resources to provide 24/7 Registration Authority Support with the rollout of Cerner Millennium

- individuals will be identified from within the Trust, to act as Registration Authority Agents and Registration Authority Sponsors

- inside core hours, users will telephone the Information Technology Service Desk for support

- outside core hours, users will telephone a single point of contact at the Trust for support.

10.3 Services provided by the Local Registration Authority Support team will include:

- registration of new users

- revocations

- personal Information Number/Passcode changes

- smartcard unlocking

- issuing new cards to replace cards lost, stolen, damaged or expired are dealt with by the Registration Manager / Team on receipt of a DATIX submission.

11. LOCAL AUDIT

11.1 All Registration Authority policies, processes and procedures will be auditable by internal auditors as well as external auditors. Audits would typically cover:

- issuance of Smartcards

- management of Smartcards

- profiles associated with users in relation to what they do

- use of Smartcards
- use of National applications
- identity management
- security of supplies and equipment
- smartcards are handled securely by Users
- registration Authority documents and forms are used and stored appropriately
- access to National Applications and Records is controlled appropriately
- unused Smartcards are stored safely and appropriate records are kept
- role Based Access Control role allocation and de-allocation is performed appropriately
- random checking of Role Based Access Control roles with those requested by the sponsor

11.2 To aid audit the following records will be maintained:

- the number of Smartcards held
- details of Smartcards issued

11.3 Registration Authority Agents must retain sufficient records to be able to determine, at a later date, the supporting evidence and methods used to verify and validate identity. All of the following information must be recorded by the Registration Authority for all users registered:

- RA01 form
- the identity requirements that were met
- the unique document numbers of identity documents that contain such numbers

11.4 All these documents need to be clearly marked with the user's Smartcard number, indexed and filed in a designated area.

11.5 Accreditation of this Registration Policy will require that periodic audit of the registration practices and procedures are conducted to ensure continued compliance.

11.6 The Registration Authority Managers and Caldicott Guardian are responsible for annual audits.

12. STAFF AWARENESS

General Awareness

12.1 A vital component to the success smart cards maintenance is raising staff awareness about cards, usage and procedures. Therefore it is a requirement for the Trust Registration Authority to work closely with all communications channels to provide an effective means of raising staff awareness.

12.2 This will include:

- roles and responsibilities
- what the cards are for
- rules and procedures
- accessing the systems
- security and confidentiality

Security and Confidentiality

12.3 Card holders will be made aware of the issues surrounding the correct use of cards, for example:

- not sharing Smartcards, Passcodes or Personal Information Numbers
- keep Personal Information Numbers and Smartcards secure
- what to do if a suspected loss or security breach occurs

13. TRAINING REQUIREMENTS

13.1 The Trust Registration Authority Team members include Registration Authority Managers, Registration Authority Sponsors and Registration Authority Agents. There is a requirement to formally train all Registration Authority staff on the utilisation of National Personal Information Number Systems (Personal Information Number User Directory and Card Management Service) and on National Policy and Procedures.

13.2 The type of training required will be based on the team member's level of responsibility within the Trust Registration Authority.

14. INTER TRUST AGREEMENTS

14.1 Agreements may be entered into with other NHS Trusts, Primary Care Trust's and General Practitioner Practices regarding shared services, Consultants and non-NHS employees and cross boundary working. It is important that these agreements are signed off by the Trust Board and reviewed by the Trust Registration Authority Team to ensure compliance.

15. EQUALITY IMPACT ASSESSMENT

15.1 All relevant persons are required to comply with this document and must demonstrate sensitivity and competence in relation to the nine protected characteristics as defined by the Equality Act 2010. In addition, the Trust has identified Learning Disabilities as an additional tenth protected characteristic. If you, or any other groups, believe you are disadvantaged by anything contained in this document please contact the Equality and Diversity Lead who will then actively respond to the enquiry.

16. MONITORING COMPLIANCE AND EFFECTIVENESS

Monitoring arrangements for compliance and effectiveness

16.1 The Trust will utilise the Information Governance Toolkit and related national initiatives, e.g. CQC for ongoing monitoring against information governance data quality standards.

Responsibilities for conducting the monitoring

16.2 The Caldicott and Information Governance Group will monitor overall compliance against registration authority standards. Assessment reports of compliance will be produced by the Registration Authority lead and presented to the Caldicott and Information Governance Group along with, where required, compliance work plan.

16.3 **Methodology to be used for monitoring**

- Information Governance Toolkit
- Incident reporting
- Audits

17. COUNTER FRAUD

17.1 The Trust is committed to the NHS Protect Counter Fraud Policy – to reduce fraud in the NHS to a minimum, keep it at that level and put funds stolen by fraud back into patient care. Therefore, consideration has been given to the inclusion of guidance with regard to the potential for fraud and corruption to occur and what action should be taken in such circumstances during the development of this procedural document.

18. RELEVANT CARE QUALITY COMMISSION (CQC) REGISTRATION STANDARDS

18.1 Under the **Health and Social Care Act 2008 (Regulated Activities) Regulations 2014 (Part 3), the fundamental standards** which inform this procedural document, are set out in the following regulations:

(please remove any of the below which are not considered relevant to the policy you are developing)

Regulation 11:	Need for consent
Regulation 12:	Safe care and treatment
Regulation 13:	Safeguarding service users from abuse and improper treatment
Regulation 17:	Good governance
Regulation 19:	Fit and proper persons employed
Regulation 20:	Duty of candour
Regulation 20A:	Requirement as to display of performance assessments.

18.2 Detailed guidance on meeting the requirements can be found at http://www.cqc.org.uk/sites/default/files/20150311%20Guidance%20for%20providers%20on%20meeting%20the%20regulations%20FINAL%20FOR%20PUBLISHING.pdf

Relevant National Requirements

Department of Health – Information Governance Toolkit

Data Protection Act 1998

NHS Records Management: Code of Practice 2005

19. REFERENCES, ACKNOWLEDGEMENTS AND ASSOCIATED DOCUMENTS

19.1 **References**

Information Governance Toolkit version 13

19.2 **Cross Reference to other procedural documents**

Confidentiality and Data Protection

Data Quality Strategy

Disciplinary Policy

Information Security Policy

Record Keeping and Records Management Policy

Untoward Event Reporting Policy and procedure

All current policies and procedures are accessible in the policy section of the public website (on the home page, click on 'Policies and Procedures'). Trust Guidance is accessible to staff on the Trust Intranet.

20. APPENDICES

12.1 For the avoidance of any doubt the appendices in this policy are to constitute part of the body of this policy and shall be treated as such.

Appendix A Nominated Sponsors and Agents

APPENDIX A

Nominated Sponsors & Agents for Somerset Partnership NHS Foundation Trust

Sponsors: Matrons from all Community Hospitals.

Line Managers of all Departments.

Agents: Nominated Personnel from all areas, generally Administration & Clerical staff (see attached current list).

CHAMPION USERS FOR COMMUNITY LOCATIONS

These members of staff have the ability to reset / unlock Smartcards.

BRIDGWATER:	Chere Turberville	01278 – 436788
	Luisa Stephens	01278 - 436795
MALLARD COURT	Lucy Drewett	01278 – 436712
	Kirsty Disney	01278 - 432041
BURNHAM:	Kay Emery	01278 – 773100
	Bridget Nevay	01278 - 773100
MINEHEAD:	Vanessa Singer Saunders	01643 - 707251
	Marissa Otero Perez	01643 - 701707
WILLITON:	Lynne Stokes	01984 - 635600
WELLINGTON:	Helen Fouracre	01823 – 662663
DENE BARTON:	Carron Scott	01823 - 431930
CHARD:	Gillian Wallace	01460 - 238231
WEST MENDIP:	Jeanette Watson	01458 - 836450
	Alyson Rees	01458 - 836450
SHEPTON MALLET:	Sarah Chaplin	01749 – 342931
	Pauline Ashford	01749 - 341103
FROME:	Toni Waller	01373 – 454747
	Simone Osborne	01373 – 454747

13.04.15