NHS
Cheshire and Wirral Partnership
NHS Foundation Trust

Document level: Trustwide (TW)
Code: HR13
Issue number: 4

Registration Authority (RA) Operational Policy

Lead executive	Director of Director of People OD
Authors details	Registration Authority (RA) Manager - 01244 393111

Type of document	Policy
Target audience	All CWP staff including staff in partner organisations, using systems which require Smartcard authentication
Document purpose	Outline policy / procedure for management of Smartcards. The NHS Smartcard is a card containing an electronic chip (similar to a chip and PIN credit card) that is used to access the NHS Care Records System, Electronic Staff Record and other applications. The chip does not contain any personal information. The combination of the NHS Smartcard and Passcode together provide high levels of security and confidentiality for all patient and staff data.

Approving meeting	Information and Data Protection Sub Committee	Date 15/01/2019
Implementation date	January 2019 followed by an annual compliance review	

CWP documents to be read in conjunction with	
HR6	Mandatory Employee Learning (MEL) policy
HR3.3	Trust disciplinary policy and procedures
GR1	Incident reporting and management policy

Document change history	
What is different?	1. Addition of Smartcard Self-Unlock facility 2. Addition of responsibility of managers to ensure staff register for the Smartcard Self-Unlock facility 3. Addition of responsibility of all smartcard user to register for the Smartcard Self-Unlock facility 4. Update of all document links and email addresses 5. Update of RISG to IGDP (Information Governance and Data Protection Sub Committee)
Appendices / electronic forms	1. Appendix 1 - Obtaining a Smartcard – New Starter 2. Appendix 2 – Obtaining a Smartcard – External Provider 3. Appendix 3 - Closing or Revoking Smartcard Access 4. Appendix 4 - Incident Grading Matrix
What is the impact of change?	Low

Training requirements	Training requirement for this policy are as stipulated within; 1. National Registration Authority Policy 2014; and 2. National Registration Authorities Operational and Process Guidance 2016.

Document consultation	
Clinical Services	Who within this service have you spoken to
Corporate services	Who within this service have you spoken to

External agencies	Who within this service have you spoken to

Financial resource implications	None

External references
1. NHS Operating Framework 2013/14
2. National Registration Authority Policy (Sept 2014)
3. Registration Authorities Operational and Process Guidance V5.2 18/02/2016
4. NHS Care Record Guarantee (2011)
5. The NHS Confidentiality Code of Practice (2003)
6. NHS Records Management Code of Practice for Health and Social Care 2016
7. NHS Employers – Identity Checks Standard (Sept 2017)
8. IG Toolkit (IGT)
9. Data Protection Act 1998

Equality Impact Assessment (EIA) - Initial assessment	**Yes/No**	**Comments**
Does this document affect one group less or more favourably than another on the basis of:		
- Race	No	
- Ethnic origins (including gypsies and travellers)	No	
- Nationality	No	
- Gender	No	
- Culture	No	
- Religion or belief	No	
- Sexual orientation including lesbian, gay and bisexual people	No	
- Age	No	
- Disability - learning disabilities, physical disability, sensory impairment and mental health problems	No	
Is there any evidence that some groups are affected differently?	No	
If you have identified potential discrimination, are there any exceptions valid, legal and/or justifiable?		
N/A		
Is the impact of the document likely to be negative? - If so can the impact be avoided? - What alternatives are there to achieving the document without the impact? - Can we reduce the impact by taking different action?	No N/A N/A N/A	
Where an adverse or negative impact on equality group(s) has been identified during the initial screening process a full EIA assessment should be conducted. If you have identified a potential discriminatory impact of this procedural document, please refer it to the human resource department together with any suggestions as to the action required to avoid / reduce this impact. For advice in respect of answering the above questions, please contact the human resource department.		
Was a full impact assessment required?	No	
What is the level of impact?	Low	

Do not retain a paper version of this document, always view policy / guidance documents from the desktop icon on your computer

Contents

Do not retain a paper version of this document, always view policy / guidance documents from the desktop icon on your computer

1. Introduction

A Registration Authority (RA) manages Smartcards and the registration and access control processes. The role of an RA is to ensure all users of National Programme applications are provided with the appropriate levels of access through the Smartcard system and have their identity rigorously checked. The RA at Cheshire and Wirral Partnership NHS Foundation Trust (hereafter referred to as CWP) comprises of the RA Manager, RA Advanced Agents, RA Agents and Local Smartcard Administrators.

As more national applications and clinical systems are released, the RA function and the NHS smartcard plays an increasingly vital role in the continued development of information security and patient care.

The process of gaining access to these National Applications, e.g. e-Referral (formerly Choose & Book), Summary Care Records, is carried out by the Registration Authority using an Integrated Identity Management (IIM) interface, which combines the benefits of the Electronic Staff Record (ESR) with the RA's system 'Care Identity Service' (CIS).

The registration process applies nationally and must meet the current Government requirements.

All the National Programme applications use a common security and confidentiality approach. Access levels are identified in terms of organisation code(s), role code(s), and business function(s).

The method by which users will be able to access a National application is via a Smartcard issued either during the ID appointment for new employees (part of the recruitment process) or by appointment for internal access requests. Both instances are managed by the People Information team at CWP with support from the Recruitment team for new starters.

The combination of the NHS smartcard and passcode together provide high levels of security and confidentiality for all patient and staff data. Once an applicant has been successfully registered, they will have a smartcard with User Unique Identifier (UUID) and a PIN number, which will permit their access to the appropriate application/s and information.

The NHS RA policies require that the only party who can authorise the setting up of roles for staff to access NHS information held by a trust is the trust themselves. Any access granted is time limited by the certificates applied to the smartcard which requires renewal every two years.

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

2. Aims

This document describes procedures for the operation of the Registration Authority (RA) and Smartcards within CWP.

With delegated responsibility from NHS Digital (formerly HSCIC), the Registration Process is operated at a local level by a Registration Authority (RA). The Trust will comply fully with the latest published National Policies and Procedures identified in the following documents:

- National Registration Authority Policy (Sept 2014)
- NHS Employers - Identity Checks (Sept 2017)
- Registration Authorities Operational and Process Guidance V5.2 18/02/2016
- The NHS Confidentiality Code of Practice (2003)

Do not retain a paper version of this document, always view from the website www.cwp.nhs.uk to ensure it is the correct version

- NHS Operating Framework 2013/14
- NHS Care Record Guarantee (2011)
- IG Toolkit (IGT)
- NHS Records Management Code of Practice for Health and Social Care 2016
- Data Protection Act 1998 – a guide from the ICO (Information Commissioner's Office)

3. Scope

This policy applies to all those working in the Trust, in whatever capacity. Failure to follow the requirements of the policy may result an investigation being conducted, which may lead to further management action being taken as considered appropriate.

This may include formal action in line with the CWP's Disciplinary or Capability policies for Trust employees and other action in relation to other workers, which may result in the termination of an assignment, placement, secondment or honorary arrangement. Non-compliance may also lead to criminal action being taken.

This document will be published on the CWP website and made known to all Smartcard users.

4. Abbreviations

CIS	Care Identity Service
CRS	Care Records Services
ESR	Electronic Staff Record
IIM	Integrated Identity Management
ICO	Information Commissioner's Office
LSA	Local Smartcard Administrator
PBAC	Position Based Access Control
RA	Registration Authority
IGDP	Information Governance and Data Protection Sub Committee
URP	User Responsibility Profile e.g. Supervisor Self Service
UUID	User Unique Identifier (on a Smartcard)

5. Key forms / documents

The following forms / documents are referenced within this policy and they facilitate the timely and accurate provision of Smartcards and relevant access, all being available via the CWP intranet site: -

- Employee Systems Access Checklist
- ESR Non-Employee Record Request Form – External Provider
- ESR System Admin URP User Access Form
- Smartcard Leaflet

6. Roles and Responsibilities

6.1 Registration Authority

Do not retain a paper version of this document, always view from the website www.cwp.nhs.uk to ensure it is the correct version

CWP has a governance structure in place which enables it to ensure that individuals providing healthcare services to the NHS directly, or indirectly, have access to NHS CIS compliant applications/information only as necessary to undertake their workplace role.

All individuals wishing to register to use the NHS CIS must be e-GIF Level 3 compliant, a government set standard for identification authentication.

The role of RA within CWP will be undertaken by the People Information team, reporting to the IGDP.

The table below provides an overview of the Care Identity Service RA roles and business functions:

CIS RA Role Name	Overview of Responsibilities
RA Manager	Overall responsibility for local RA processes and governance
Advanced RA Agent	Has the ability to action nearly all of the RA processes available to the RA Manager except assign register users to the RA roles in their own organisation and assign RA Managers in child organisations that are RA hosting
RA Agent	Main function is to grant requests
Local Smartcard Administrator	Has the ability to unlock Smartcards and assist in the renewal of certificates

Further, detailed information about each RA role's functions is outlined in sections 6.2 to 6.5.

6.2 Registration Authority Team

The RA team is responsible for policy development and ensuring policy compliance in all aspects of RA activity. The team forms part of the People Information team within People Services (with the exception of the Caldicott Guardian who is not part of the People Information team) and comprises:

- Director of People Services;
- Caldicott Guardian;
- RA Managers;
- RA Advanced Agents / RA Agents;
- Local Smartcard Administrators.

The RA team is responsible for ensuring that:

- National Registration processes are adhered to in full;
- Any local processes developed to support the National Registration processes are adhered to in full;
- Appropriate forms requesting access are used correctly;
- There is sufficient availability of resource to operate the registration processes in a timely and efficient manner and there are sufficient Smartcards and Smartcard issuing and maintenance equipment for the organisation;
- That the People Information team members are adequately trained and familiar with the local and national RA processes;
- An indexed and secure audit trail is maintained of applicants' registration information and profile change requests;
- All completed application forms and associated documents are kept secure in an area, in line with NHS Records Management Code of Practice for Health and Social Care 2016;
- People Information team members are familiar with - and understand - RA policy and practices;

Do not retain a paper version of this document, always view from the website www.cwp.nhs.uk to ensure it is the correct version

- RA Advanced Agents, RA Agents and Local Smartcard Administrators are familiar with and understand their roles and are fully trained;
- Notifications of the creation and revocation of RA managers.

6.3 Registration Authority Manager

The RA manager is responsible for ensuring the robustness, integrity and policy compliance of all aspects of CWP's RA service on a day to day basis. CWP will have no fewer than two RA managers, who will:

- Publish and maintain the list of RA members with their names, roles, contact details and areas of responsibility clearly defined on the Trust intranet;
- Assign and register RA agents (where permitted under governance arrangements), ensuring there are sufficient resources to operate the registration processes in a timely and efficient manner
- Ensure that the National Registration policy and processes identified in this document are adhered to and that any local processes support the national policy and processes;
- Identify areas where CWP business processes need integrating to minimise risk and duplication of effort. For example, HR processes for starters, leavers, suspensions, terminations, and long term absences;
- Restricting users to having only one NHS CRS Smartcard issued to them, showing their User's Unique Identifier (UUID) and photograph
- Manage the retrieval and disposal of Smartcards once staff have left the Trust
- Managing renewal of Smartcard certificates
- Ensure that there is sufficient availability of resource to operate the registration processes in a timely and efficient manner
- Ensure that a secure audit trail is maintained of applicants registration information
- Ensure line managers complete leaver forms in a timely and accurate manner in order that the card revocation process can be acted upon
- Ensure line managers are familiar with and understand systems access forms and ensure these forms are appropriately used
- Maintain adequate stock of Smartcards and RA hardware
- Ensure that all RA Printers & Smartcard Readers are properly maintained and that an audit of such equipment is carried out at regular intervals to ensure its ongoing operation
- Ensure that Identity Agent software is kept up to date on each Trust PC that requires it
- Identify areas where the Trust business processes require integration to avoid duplication. For example, HR processes for starters, leavers, suspensions, terminations
- Escalate all queries that cannot be resolved locally to the next level in the Management hierarchy
- Ensure that all Smartcard users, RA Advanced Agents, RA Agents and Local Smartcard Administrators are informed of changes to national and local RA process and procedures
- Make Smartcard users aware of their responsibilities
- Ensure Smartcard users are monitored for compliance and provide appropriate reports on compliance and non-compliance to the IGDP
- Report all RA related security incidents and breaches to the IGDP

Refer to the table below for functions available to RA Managers.

6.4 Registration Authority Agents / Advanced Registration Authority Agents

Advanced RA Agents and RA Agents are responsible to the RA managers. CWP will allocate responsibilities to nominated staff within the Informatics and People Information teams who are collectively responsible for ensuring that the national and local policies/processes are followed and for the accurate input of information on CIS.

Do not retain a paper version of this document, always view from the website www.cwp.nhs.uk to ensure it is the correct version

FUNCTIONS AVAILABLE IN CIS	RA Manager	Advanced RA Agent	RA Agent
Register RA Manager in child hosting organisation	✓	×	×
Register Advanced RA Agent, RA Agent, RA Agent ID Checker, Sponsors and Local Smartcard Administrators in own organisation and child organisations	✓	×	×
Register Smartcard users	✓	✓	✓
Search and view closed users	✓	✓	✓
Reopen closed users	✓	✓	✓
Create positions and workgroups	✓	✓	×
Modify positions	✓	✓	×
Assign individuals to positions	✓	✓	✓
Review positions definitions including assigned users	✓	✓	✓
Assign individuals to workgroups	✓	✓	✓
Manage request lists	✓	✓	✓
Access reporting and run reports	✓	✓	✓
Assign users to positions	✓	✓	×
Use batch functionality	✓	✓	×
Create Temporary Access Cards	✓	✓	✓
Cancel Smartcards	✓	✓	✓
Close user	✓	✓	✓
Unlock Smartcards & renew certificates	✓	✓	✓
View all requests	✓	✓	✓

6.5 Local Smartcard Administrators (LSA's)

Nominated LSA's are available in some areas of CWP, with the People Information team providing support for Corporate users. LSA's are able to assist staff with the items detailed in the table below;

Local Smartcard Administrator Functions in CIS
Renew Certificates (if the user has not self-renewed when prompted and therefore have expired)
Unlock Smartcards (where the user has had 3+ failed attempts to log in)

6.6 The Trust Board

RA Managers & Sponsors are appointed by CWP and this appointment is confirmed in a letter of appointment which must be held by each individual appointed to these positions. Copies of these letters should also be held by the RA Manager so they are able to provide the necessary evidence to meet IG Toolkit requirements.

Notification of the creation and revocation of RA managers (including their e-mail address) should be sent to ramanagers.agents@hscic.gov.uk

Do not retain a paper version of this document, always view from the website www.cwp.nhs.uk to ensure it is the correct version

6.7 Caldicott Guardian

The Caldicott Guardian (Medical Director and Responsible Officer : Effectiveness & Workforce) will consider incidents reported to him via the IGDP and advise on whether CWP systems or working practices are required to be reviewed as a result.

6.8 Information Governance and Data Protection Sub Committee (IGDP)

The IGDP is a formal working group, whose duties include overseeing and coordinating the technical and organisational security measures that need to be place for all the key Information assets. This ensures the confidentiality, integrity and availability of information and complies with the ISO 27001 Information Security Standard.

The group will consider incidents reported to them and decide whether Trust systems or working practices should be reviewed as a result. The group will escalate incidents through the Risk Management Structure where appropriate.

6.9 Human Resources

It is the responsibility of the Human Resources department to ensure:

- Reported incidents involving smartcard misuse or security issues are investigated and disciplinary action taken where deemed appropriate.
- In addition to ensuring that a Datix incident has been registered, any such issues are reported to the RA Manager as soon as they are identified in order that the People Information team can include this information in their quarterly reports to the IGDP for audit and compliance purposes.

6.10 Line Managers

It is the responsibility of line managers to ensure compliance with the following:

- When recruiting to a post, ensure that the advert details in CWP's recruitment system (TRAC), includes whether the role requires a Smartcard or not.
- As soon as possible after making a conditional offer of employment, ensure that an Employee Systems Access Checklist is fully completed and emailed from their email address to cwp.peopleinformation@nhs.net . This will be emailed to them via TRAC. Failure to do so will result in an ineffective ID appointment with a Smartcard not being issued and a further face to face appointment will be necessary with the prospective new employee.
- Communicate a start date for prospective new employees as soon as the Recruitment Team confirm that all pre-employment checks are cleared. This will in turn enable the People Information team to provide timely access to all locked Smartcards that have been issued on the confirmed start date.
- For all staff name changes:
    i. Ensure all changes are confirmed in ESR via Supervisor Self Service, having viewed necessary documentation (e.g. deep poll, decree nisi, marriage / civil partnership documents) to satisfy themselves that the change is valid.
    ii. For staff who are Smartcard users, follow the steps in point i above and ensure they are then directed to the People Information Team, who will take necessary steps to issue a new Smartcard via a face-to-face appointment.
- For all internal staff movements, ensure that the Employee Systems Access Checklist is completed and sent to cwp.peopleinformation@nhs.net The relevant ID documents will need to be produced again at this appointment.
- Ensure the timely completion of all leaver forms and change forms in order that ESR can notify the People Information team, who will take necessary steps to amend/revoke access to Smartcard access as appropriate.

Do not retain a paper version of this document, always view from the website www.cwp.nhs.uk to ensure it is the correct version

- Ensure timely and accurate completion of Attendance Line in order that Smartcard access can be revoked for those on long term sickness absence and re-associated upon their return, as notified by ESR.
- Ensure that any incidents involving smartcard misuse or security issues are reported to the RA Manager, the relevant line manager and a Datix incident raised;
- Ensure Smartcard users who they are accountable for comply with the requirements as detailed in section 6.12.
- Ensure all smartcard users they are responsible for register for the Smartcard Self-Unlock facility.

6.11 Informatics Service Desk

It is the responsibility of the Informatics Service Desk to ensure compliance with the following:

- That all employees' computers comply with all software / hardware / configuration requirements in order that Smartcard users are able to access the relevant applications required, in line with the latest advice from NHS Digital and any updates provided by the People Information team;
- To assist employees with the re-setting of their Smartcard PIN / Passcode. In such instances, to always check the identity of the caller by asking them to confirm either of the following 2 items before proceeding, both of which are available via their named record on the Spine:
    i. Their date of birth
    ii. Their National Insurance Number

6.12 All Users of the RA Service

A Smartcard is a national token of a user's identity and users therefore have a duty to keep patient information secure and confidential at all times. The Smartcard provides access at the appropriate levels to healthcare information required in order that users can carry out the duties associated with their role.

All access to patient data using a Smartcard is auditable. As such, users will be accountable for all actions that are undertaken using their Smartcard which has been issued specifically only to them and only for their use during their day to day work. Each Smartcard user must:

- Comply fully with the:
    - Latest published National Policies and Procedures identified under section 2;
    - Adhere to local policies and procedures;
    - Undertake Information Governance training each year.

- Electronically accept the RA terms and conditions when first issued with a Smartcard and periodically thereafter when requested to do so.
- Renew certificates on their Smartcards when prompted to do so.
- In instances where there is a name change (e.g. due to marriage, divorce, change via deep poll etc), the user must:
    - Provide relevant ID documentation to their line manager as proof of the name change (e.g. marriage certificate, decree nisi, deed poll) in order that they can amend their record via ESR Supervisor Self Service;
    - Contact the People Information team on 01244 393107 in order that an appointment can be made to issue a new card with their new name at a face-to-face appointment. The relevant ID documents will need to be produced again at this appointment.

- Ensure lost or stolen Smartcards are:
    - Reported as soon as possible to the relevant line manager, and;
    - Reported to the People Information team; and;

Do not retain a paper version of this document, always view from the website www.cwp.nhs.uk to ensure it is the correct version

- o A Datix Incident raised.

The RA (People Information Team) will cancel the lost/stolen card and arrange a re-issue, upon consultation with the employee and/or line manager.

- Not use a Smartcard to prove NHS identity.
- Ensure the security of their cards, and not share the physical Smartcard or the confidential Passcode with anyone, nor are they to leave their card unattended at any time.
- Ensure their Smartcard is kept in a safe and secure place when not in use e.g. a locked drawer or secure locker and never to be left logged in.
- Ensure that they have their card available in work. It is recognised that some users work at multiple bases and may need to take their cards home.
- If the user forgets their card it is their responsibility to make alternative arrangements. It is recommended that the user returns home to retrieve their card and make the hours up at a later date. If this is not possible the user should take alternative tasks that do not require a Smartcard.
- A user taking an extended period of absence, i.e. longer than 3 weeks, will have their access removed until they return.
- A summary of the key points are found in the Smartcard Leaflet, which is provided to all smartcard users following registration and is available on the Smartcard intranet page, reminding smartcard users of their responsibilities and obligations.
- Register for the Smartcard Self-Unlock facility.

7 Training

The RA Manager is accountable for all staff holding RA roles within CWP and must ensure appropriate training is completed by the following groups:

- All staff who are either RA Advanced Agents, RA Agents or Local Smartcard Administrators must complete local RA training as instructed by the Trust's RA Manager.
- In addition, the National Registration Authority and Smartcard Policy e-learning module must also be completed as instructed by the Trust's RA Manager and can be accessed via ESR e-learning.
- All smartcard users must receive relevant guidance or training before accessing any local or national application for the first time. It is the user's responsibility to ensure they have received suitable guidance before accessing any spine or non-spine based application via their smartcard.

8 Service Availability

The People Information team are able to deal with all RA support issues (except where the issue is an IT issue) and will be available during core hours of 09:00hrs – 17:00hrs Monday to Friday (excluding bank holidays).

In order to support staff with Smartcard issues, and in order to minimise unnecessary travel for users, the Informatics team are able to remotely log onto staff computers to assist with certain issues that may arise. In addition, Local Smartcard Administrators in some areas are able to assist with certain issues also - refer to the table below and / or the Smartcard Leaflet for further information:

Issue	Relevant RA / Dept
PIN / Passcode re-setting	• Informatics team (Servicedesk) • People Information team
Renewal of Certificates	• Local Smartcard Administrator (see Smartcard Leaflet)

Do not retain a paper version of this document, always view from the website www.cwp.nhs.uk to ensure it is the correct version

	• People Information team
Unlock smartcard	• Informatics (see Smartcard Leaflet) • People Information team
Name Change	• People Information dept (via appointment only)

The services of the RA outside of core hours should be considered as emergency only and should only be requested when waiting until core hours would be detrimental to patient care or confidentiality. In such circumstances the service is required to implement their local Business Continuity Plans (BCP) until core hour service is resumed.

9. Incident reporting

Incidents can be reported by any member of staff where they feel that there is a risk to patient health, confidentiality or CWP reputation. Incidents should be reported using the Incident Reporting and Management Policy to the RA managers, in addition to informing their line manager and the Human Resources team. Examples of incidents are:

- Smartcard or application misuse;
- Non-compliance of local or national RA policy;
- Any unauthorised access of Smartcard applications;
- Any unauthorised alteration of patient data;
- Lost, stolen or damaged cards.

Any incidents considered significant must be reported to an RA Manager. A major breach of security will also be reported in accordance with the CWP Incident Reporting and Management Policy

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.

Incidents involving breaches of security or demonstrate that a user may not be considered trustworthy should always be reported to the appropriate RA manager, who will ensure that the appropriate investigation and action takes place. The RA manager will notify the relevant managers.

Incidents relating to reporting failure or unavailability of Smartcard applications may be reported by any member of staff by ringing the Informatics Servicedesk on 0300 303 8182 or emailing servicedesk@cwp.nhs.uk

RA Advanced Agents, RA Agents or RA Administrators will report any RA related incidents, using the CWP Incident Reporting and Management Policy procedure to the RA Manager. Additionally RA staff will report any operational difficulties, especially where these have patient healthcare implications, to People Information.

10. Management of Systems Access

All access requests are required to be provided in writing from the relevant line manager for audit purposes. At CWP, Smartcards are used to access various clinical systems, as well as for managers to access ESR Manager / Supervisor Self Service. Therefore, a robust system of requesting / revoking access has been implemented:

11. Creation of a Digital Identity

11.1. ID Appointment Process

Do not retain a paper version of this document, always view from the website www.cwp.nhs.uk to ensure it is the correct version

All new starters, whether new to CWP or existing staff who have secured a new role within CWP, must comply with the ID appointment process, which requires them to attend CWP's Trust Board offices on one occasion to provide all necessary ID. Both the Recruitment and People Information teams will carry out all necessary actions during this one ID appointment. Refer to;

Appendix 1 - Obtaining a Smartcard – New Starter and

Appendix 2 – Obtaining a Smartcard – External Provider

In order for the ID appointment process to be successful, both teams will rely on the recruiting manager for the following:

a. Having confirmed whether a smartcard is required for the role at the point of advertising or not, and;

b. Having forwarded a completed Employee Systems Access Checklist to the People Information team as soon as possible after making a conditional offer of employment.

Following a conditional offer of employment having been made by the recruiting manager, CWP's recruitment system TRAC, instigates the following 2 initial processes:

a. The applicant will be invited to attend an ID appointment within the following 2 weeks.

b. The recruiting manager will receive an email via TRAC stating that they are required to complete the Employee Systems Access Checklist for the applicant in question. It is vital that this form is completed in full and received prior to the applicant attending their ID Appointment as it informs the People Information team what access is required for this role.

Failure to complete the Checklist and/or ensure it is provided prior to the ID appointment will potentially result in a failed ID Appointment, requiring the applicant to visit the People Information team a second time, rather than completing all actions at the first appointment.

The applicant will then attend their ID appointment, which is split into 2 parts:

a. The Recruitment team will firstly carry out all necessary recruitment ID document checks, ensure relevant information is input into TRAC and ESR and continue to chase all other pre-employment checks such as references, Occupational Health clearance etc.

b. Where a recruiting manager has indicated that the applicant will require a smartcard, they will be escorted to the People Information team, where they will carry out further ESR checks, take a photo and issue the Smartcard.

The Smartcard will, on some occasions, be issued locked (i.e. with no access on it) until ESR confirms via a new starter / change notification to the People Information team that the applicant has been hired into post. In such instances, the new employee or their manager should contact the People Information team on 01244 393107 once they have started in post, who will then arrange to remotely associate the employee's Smartcard with the access requested.

For existing staff moving roles, all the above steps apply in full. However, where an employee already has a Smartcard and all ID documents are already in ESR, the process will be much quicker and requirements will be advised on an individual basis. An Employee Systems Access Checklist must however still be completed in all cases.

11.2 Acceptable Forms of Identity Documentation

To ensure compliance with the Registration Authorities Operational Processes and Guidance and the NHS Employers – Identity Checks Standard (Sept 2017), the Registration Authority must follow nationally agreed processes as detailed in section 6.2, including that all Smartcard users/applicants must provide either:

Do not retain a paper version of this document, always view from the website www.cwp.nhs.uk to ensure it is the correct version

a. Two forms of personal photo ID and one proof of address; or
b. One form of personal photo ID and two proof of address documents. A National Insurance Number should also be available at registration.

11.3 Acceptable Photo Personal Identity Documents

- Full, signed UK (Channel Islands, Isle of Man or Irish) passport or
- EU/other nationalities passport
- UK Biometric Residence Permit (BRP) card
- UK full or provisional photo card driving licence
- EU/other nationalities photo card driving licence (valid up to 12 months up to the date of when the individual entered the UK and providing that the person checking is confident that non-UK photo card driving licences are bona fide).
- HM Armed Forces Identity card (UK)
- Identity cards carrying the PASS (Proof of Age Standards Scheme) accreditation logo (UK and Channel Islands).

Organisational identity cards are not acceptable as they do not contain watermarks, holograms or other security markings.

Any document not listed above is NOT acceptable.

11.4 Acceptable Proof of Address Documents

To confirm address, various documents are acceptable as detailed in NHS Employers – Identity Checks Standard (Sept 2017)

11.5 No Acceptable Photographic Documentation Available

If the applicant is unable to provide acceptable photographic personal identification, two forms of non-photographic personal identification and three documents confirming the address must be provided. All five documents must be from different sources. To confirm personal identification, various documents are acceptable as detailed in NHS Employers – Identity Checks Standard (Sept 2017).

In addition the applicant will need to provide a passport sized photograph, endorsed on the back with a signature by a 'person of standing' in the community who has known them for at least two years.

A 'person of standing' could be a magistrate, medical practitioner, officer of the armed forces, teacher, lecturer, lawyer, bank manager or civil servant.

The photograph should be accompanied by a signed statement from the person of standing, indicating the period of time that they have known the applicant. The statement also needs to contain a legible name, address and telephone number of the person of standing.

Where the User is unable to provide appropriate identification they will not be issued with a Smartcard and will not be permitted access to national applications.

12 Employee Systems Access Checklist

The People Information team will ensure that latest version of the Employee Systems Access Checklist is used and published on the intranet.

All line managers will be made aware that the Employee Systems Access Checklist is to be completed to arrange access to various systems operated within CWP which require a smartcard. The Checklist may also be used for internal staff who require specific access but are not moving roles.

Do not retain a paper version of this document, always view from the website www.cwp.nhs.uk to ensure it is the correct version

12.1 ESR System Admin URP User Access Form

A link on the Employee Systems Access Checklist directs a manager to the ESR System Admin URP User Access Form, which is to be completed when an employee requires access to any URP (User Responsibility Profile) within ESR e.g. Manager / Supervisor Self Service (SSS).

e-Learning and Employee Self Service are automatically provided to all CWP staff. For external staff, this access is provided manually where appropriate.

12.2 Non-CWP Employees

Access to CWP systems may be granted to non-CWP employees e.g. staff employed by Social Services / other outside organisations, contractors, locums, agency staff etc who work as part of a team with CWP and will be subject to this policy. Refer to Appendix 2 – Obtaining a Smartcard – External Provider

All non-CWP staff who are provided with any access to any systems will be subject to the same obligations as CWP staff and any misuse of cards will be handled in line with CWP 's Disciplinary policy and procedures.

Access provision will depend on what systems are requested and the table below details which access request forms require completion by the line manager in each instance:

Form to be Completed *(all available via the People Services intranet home page)*	**Access Required:**		
	e-Learning	**SSS**	**Clinical Systems**
ESR Non-Employed Record Request Form – External Provider *(requests the creation of a basic ESR Employee Record)**	✓	✓	✓
ESR System Admin URP User Access Form *(requests access to URP's in ESR e.g. MSS, SSS etc)*	✓	✓	×
Employee Systems Access Checklist *(confirms which systems access is required)*	×	×	✓

* *Where a basic record on ESR is to be set up for an external staff member, a nominated CWP guarantor is required for each person, whose responsibility it will be to ensure the People Information team are informed of any changes to the external staff member's access status, either personal or contractual which may impact on their access requirements e.g. if they leave, change their job, change their name etc. A report detailing all external staff is provided to all CWP guarantors every 6 months for verification and governance purposes.*

13 Leavers

All Trust access positions/role profiles in the RA System pertaining to the employee must be removed as soon as is practical. Refer to Appendix 3 – Closing or Revoking Smartcard Access.

CWP operates a real time interface into ESR. As such, access to any CWP Smartcard enabled systems will be auto-revoked on the termination date.

Do not retain a paper version of this document, always view from the website www.cwp.nhs.uk to ensure it is the correct version

It is the responsibility of the line manager to clearly state on the leaver form whether the user is leaving the NHS permanently or joining another NHS organisation. Thereafter, the line manager must consider the actions to be taken relating to the Smartcard, which will differ accordingly: -

- If the user is transferring to another NHS related employment the user should to **retain the Smartcard**. Access to all CWP Smartcard-enabled applications will be revoked automatically upon termination of their assignment.
- In the event of a user permanently leaving an NHS related employment, it is the responsibility of the line manager to ensure that the following actions are carried out:
  a. The smartcard is to be recovered before the member of staff leaves CWP;
  b. The line manager should then **destroy the Smartcard** by cutting it up (several cuts, including through the chip) and then dispose of it confidentially;
  c. In this instance, following notification via ESR, the People Information team will end the employee's access to all Smartcard enabled applications by closing the user's access via the Spine.

Examples of permanently leaving the NHS would include retirement, leaving for employment to a non-NHS related job or taking up full-time education.

a. In the event of a member of staff leaving with immediate effect (e.g. following dismissal) it is the responsibility of the line manager to follow steps detailed above, ensuring they recover the Smartcard from the employee prior to them leaving the premises.

14 Record retention

- Previous paper forms (RA01, RA02, RA03, RA04, RA05, RA06, RA07, RA08 and RA09) are no longer used but are required to be retained in accordance with National Registration Authority Policy Requirements and the Records Management Code of Practice for Health and Social Care 2016. The table below summarises the requirements for the retention of RA forms:

Type of Record	Minimum Retention Period	Final Action
Personnel/Human Resources records - major (e.g. Personal files, letters of appointment, contracts references, related correspondence and RA Forms)	- **6 years** after subject of file leaves service or; - Until subject's **79th birthday**, whichever is the later.	Destroy under confidential conditions

15 Revocation

15.2 Automated addition and revocation of NHS CRS access

There are other occasions when it is necessary to deactivate a Smartcard by revoking the Smartcard certificate or cancelling the card. Such reasons for this include:

- The Smartcard is lost or stolen
- There has been some other security breach associated with the Smartcard, the Smartcard certificate and/or the Smartcard Passcode
- The user is no longer employed by an NHS organisation;
- The employee assignment status changes in ESR from 'active' to another status as detailed on section 15.2;
- The employee is absent from work due to illness on a long term basis (3 weeks or more).

Do not retain a paper version of this document, always view from the website www.cwp.nhs.uk to ensure it is the correct version

Where the revocation has been requested and authorised owing to a security related event, the RA agent will deactivate the smartcard as soon as possible. The RA agent will then confirm the action to the RA Manager who will in turn confirm this action with:

- An HR Business Partner;
- The relevant Guarantor(s) / line manager

15.2 Changes to Assignment Status

When a CWP member of staff has their assignment status in ESR changed from an 'active' assignment status, 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.

Active assignment statuses are:

- Active assignment;
- Acting up;
- Internal secondment.

Other assignment statuses are listed below. A status change to any listed below will result in the automatic revocation of NHS CRS access taking place, and as such becoming Inactive:

- Assignment costing deletion;
- Career break;
- Maternity / adoption;
- Out on external secondment – paid;
- Out on external secondment – unpaid;
- Suspend with pay;
- Widow / widower;
- Active contingent assignment end;
- Suspend assignment;
- Suspend no pay;
- Suspend contingent assignment;
- Terminate assignment;
- Terminate process assignment;
- Inactive / not worked.

15.3 Smartcard access during Long Term Sickness

In addition to the above, manual intervention by the People Information team is required when an individual is absent from work due to illness for a period of 21 days or more (long term absence), when their smartcard access is manually revoked. In this case, Smartcard access will be re-associated once the employee returns to work.

- The People Information team will rely on an ESR report detailing employees' sickness statuses and access is revoked/re-associated on a weekly basis accordingly.
- This report is generated via an interface from Attendance Line into ESR, therefore it is vital that line managers input sickness information accurately and in a timely manner into Attendance Line.

15.4 Changes to an Employee's role

Whenever there is a temporary or permanent change in the way a person works, a review of the person's CIS access must be carried out. If there are significant changes to the staff member's role the relevant role profile on the Spine User Database must be requested via the People Information team. Examples of amendment changes that would necessitate such changes are changes to a person's:

Do not retain a paper version of this document, always view from the website www.cwp.nhs.uk to ensure it is the correct version

- Job title;
- Access requirements;
- Department;
- Site(s).

Revocation tasks can only be carried out by RA Team Members within the People Information Team.

Where the revocation has been requested by HR because of security related events the RA Manager will authorise the appropriate action.

Where the user is leaving the Trust's employment, refer to section 13.

16 Lost, stolen and damaged Smartcards

For any lost, stolen and damaged Smartcards, the following actions must be taken as soon as is practicable:

- Report to issue to the relevant line manager; plus
- Report the issue to the Registration Authority Manager by emailing cwp.peopleinformation@nhs.net or the Informatics Servicedesk via email servciedesk@cwp.nhs.uk
- Complete a Datix Incident Form for lost and stolen Smartcards.

The Registration Authority Manager and the People Information team will ensure appropriate steps are taken to revoke access for lost and stolen Smartcards, which will render the Smartcard useless.

In the case of damaged Smartcards, the user will be required to attend a face-to-face appointment with the People Information team in order that their identity can be verified prior to issue of a replacement card. Where the user's identity cannot be verified, they will be required to produce documentary evidence as detailed in section 11.2 and will be advised if this is necessary when arranging the appointment.

17 Smartcard Self-Unlock Facility

If a user inadvertently locks themselves out, (e.g. by using the wrong PIN 3+ times) their smartcard will be locked. Users can now resolve this themselves, providing they have registered to be able to do so.
The Smartcard Self-Unlock facility allows users to:

a. unlock their Smartcard themselves; and
b. reset their password without having to call or visit IT or the People Information team

This will in turn save time and effort and lead to less disruption of their work. The registration process is very quick – the Self-Service Unlock Leaflet provides step-by-step instructions for all users.

18 Passcode Unlocking/Changing

Users who have not registered for the Smartcard Self-Unlock facility and have forgotten their Smartcard Passcode or, suspect it may be known by another or, who have been locked out of NHS Digital Applications because of three failed login attempts, should contact their Local Smartcard Administrator or the Informatics Servicedesk on 0303 300 8182 (email servicedesk@cwp.nhs.uk) in the first instance. Refer to the Smartcard Leaflet for contact details and further information.

The Informatics Servicedesk will always ensure that they check the identity of all employees reporting any such issues by confirming the caller's date of birth or National Insurance Number, both of which will be visible to them via the employee's record on the Spine before taking any action.

Do not retain a paper version of this document, always view from the website www.cwp.nhs.uk to ensure it is the correct version

If the user is unable to resolve the issue with the Local Smartcard Administrator or the Informatics Servicedesk, the employee should contact the People Information team and arrange a time within working hours to have the Passcode unlocked or reset. The Smartcard holder must be present and confidentially set their own Smartcard Passcode.

19 Renewal of Certificates

Smartcard certificates expire two years after issue of the card and users should use the 'Self Service Portal' to re-new their own certificates. If the notifications are ignored the user will be required to contact the People Information team to renew certificates. – the meeting must be face to face and the Smartcard holder confidentially inputs their Smartcard Passcode during this process.

20 Smartcard misuse

A staff member must report suspected smartcard misuse in line with the CWP Incident Reporting and Management Policy in that a Datix Incident Form must be completed, as well as being reported immediately to the local RA manager. Depending on the severity of the allegation an investigation may be required. If it is suspected that a smartcard is being misused then it should be reported to HR who may request that the certificate associated with the smartcard be suspended or revoked as appropriate.

If smartcard misuse is alleged, an investigation must be conducted. The RA manager will consult with HR and the matter must proceed using the Disciplinary Policy and Procedure.

21 Position Based Access Control (PBAC)

PBAC links a specific job to the access rights that it requires, thereby reducing the need for access rights to be assessed on an individual basis. PBAC therefore represents an effective mechanism for providing users with the access they require in the course of their day to day work, whilst also ensuring that these access rights are properly managed and appropriate for their role.

PBAC ensures greater consistency within NHS organisations about access to care records is controlled and managed. PBAC also facilitates the management of access via the ESR interface to CIS.

CIS positions are established within CWP by the People Information team. Any new or amended positions are created subject to satisfactory approval from the relevant system lead.

Any new or amended positions will be approved and agreed ultimately by the IGDP. The People Information team will provide a summary report to the IGDP on a quarterly basis of any newly created, modified or deleted CIS positions for their review.

Once identified, the process for amendment will follow the existing authorisation process within CWP, i.e. approval will be required from the RA manager before the amendment is made to the access control position.

The amendment will be identified on the summary report of positions (ESR Master Mapping Table) which will be submitted regularly to the IGDP.

If IGDP raise any concerns, appropriate actions will be taken and recorded via the IGDP Action Log.

21.2 Removal of a PBAC

If, during the review process, the People Information team identify that an access control position is no longer required the RA Agent must identify who is currently assigned to the access control position and determine whether the staff in question need to be assigned to a new position.

Do not retain a paper version of this document, always view from the website www.cwp.nhs.uk to ensure it is the correct version

Once this has been determined it is necessary to ensure that the change is documented and included within the ESR Master Mapping Table (contained within the PBAC before the position is resubmitted to the RA Manager for approval). Upon receiving authorisation the People Information team will ensure that the ESR position linking is modified in accordance with the change.

If a replacement access control position is not required the people information team 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 People Information team will close the access control position on the Spine and ensure that it is removed from any ESR position to avoid it being assigned thereafter.

21.3 Creation of a new PBAC

A new access control position can be identified in a variety of ways as follows:

- A new NHS CRS system;
- A new ESR position within CWP;
- Identification through the review process.

When new access control positions are identified the People Information team will need to determine who requires this access and ensure that the ESR Master Mapping Table is updated.

The access control positions will be created on the Spine and associated to the relevant position in ESR.

20.3 Amendment to an ESR position

The People Information team will determine whether the ESR position in question is / is not linked to an access control position. A review must be undertaken to confirm that either:

- The current access control position is still required;
- A new access control position needs to be approved and created;
- NHS CRS access is no longer required;
- A different existing access control position is required to be linked.

If access is no longer required, the People Information team will update the ESR Master Mapping Table. The People Information team will then communicate this information to the relevant line manager, for further cascade to the staff concerned, advising them of the change.

Any anomalies will be reported to the IGDP and appropriate action taken.

20.4 Removal of an ESR position

Before an ESR position is removed the People Information team must check if it is linked to an access control position. If linking is in place the People Information team must ensure that the staff currently residing in the position are transferred into another position with the relevant NHS CRS access and the ESR Master Mapping table is updated accordingly.

22 Personal Information Management

CWP will use the ESR interface to automatically inform CIS of any personal detail changes, ensuring that the data remains aligned in both systems.

The items which will interface are:

- Title

Do not retain a paper version of this document, always view from the website www.cwp.nhs.uk to ensure it is the correct version

- Surname
- First name
- Middle name
- NI Number
- Date of Birth
- Email address
- Work phone number
- Work mobile number

22. Audit

The management and use of Smartcards will be subject to internal audit to ensure that national and local policies are being followed. Audits would typically cover:

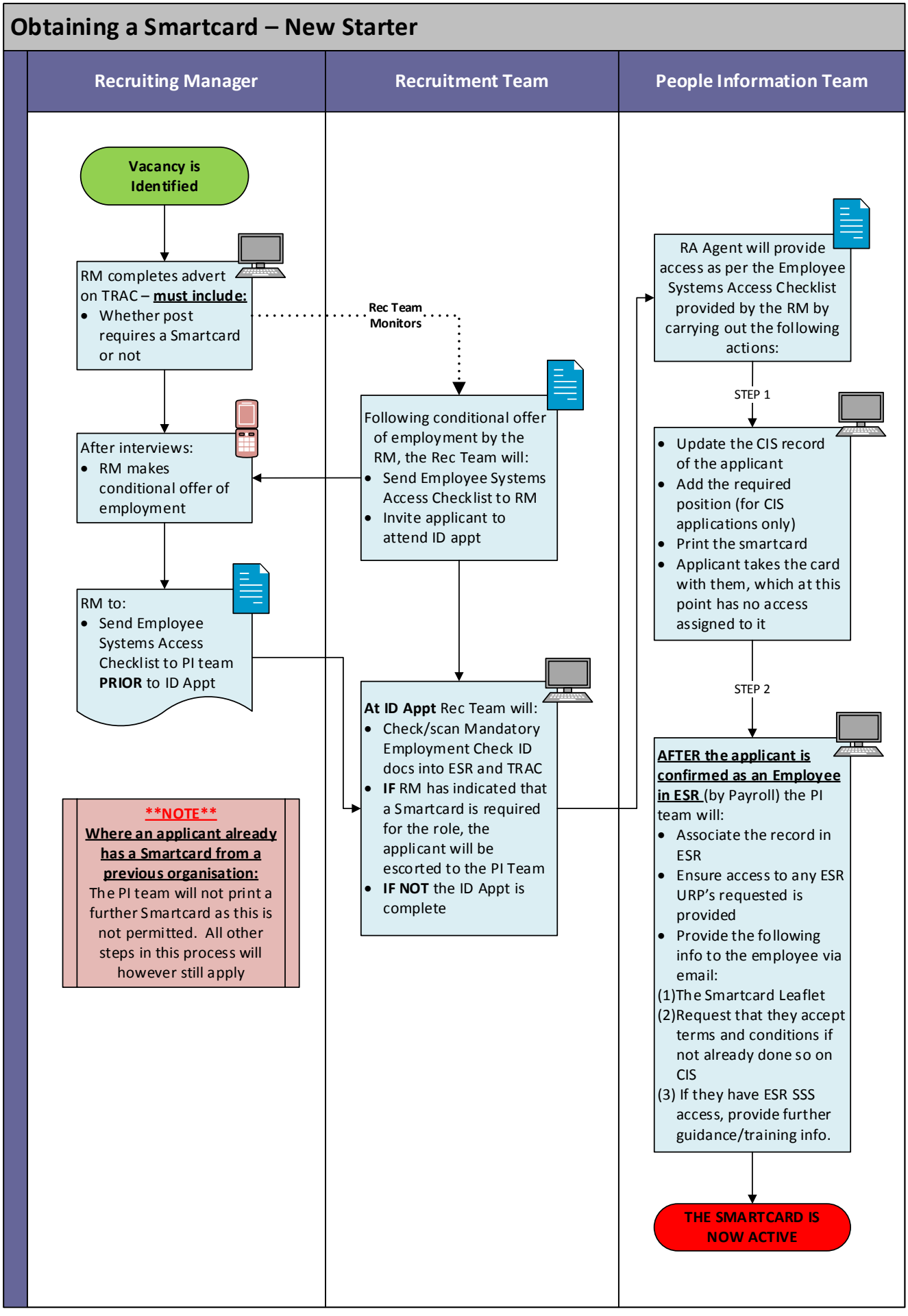
- The issue of Smartcards
- The management of Smartcards
- The profiles associated with users in relation to what they do
- The use of Smartcards
- The use of Smartcard applications
- Identity management
- Security of supplies and equipment
- RA documents are used and stored appropriately
- Access to Smartcard Applications and Records is controlled appropriately
- Unused Smartcards are stored safely and appropriate records are kept
- PBAC role allocation and de-allocation is performed appropriately

23. Reporting

To aid audit and governance requirements, a reporting schedule has been developed, which will be run and appropriate action taken as necessary.

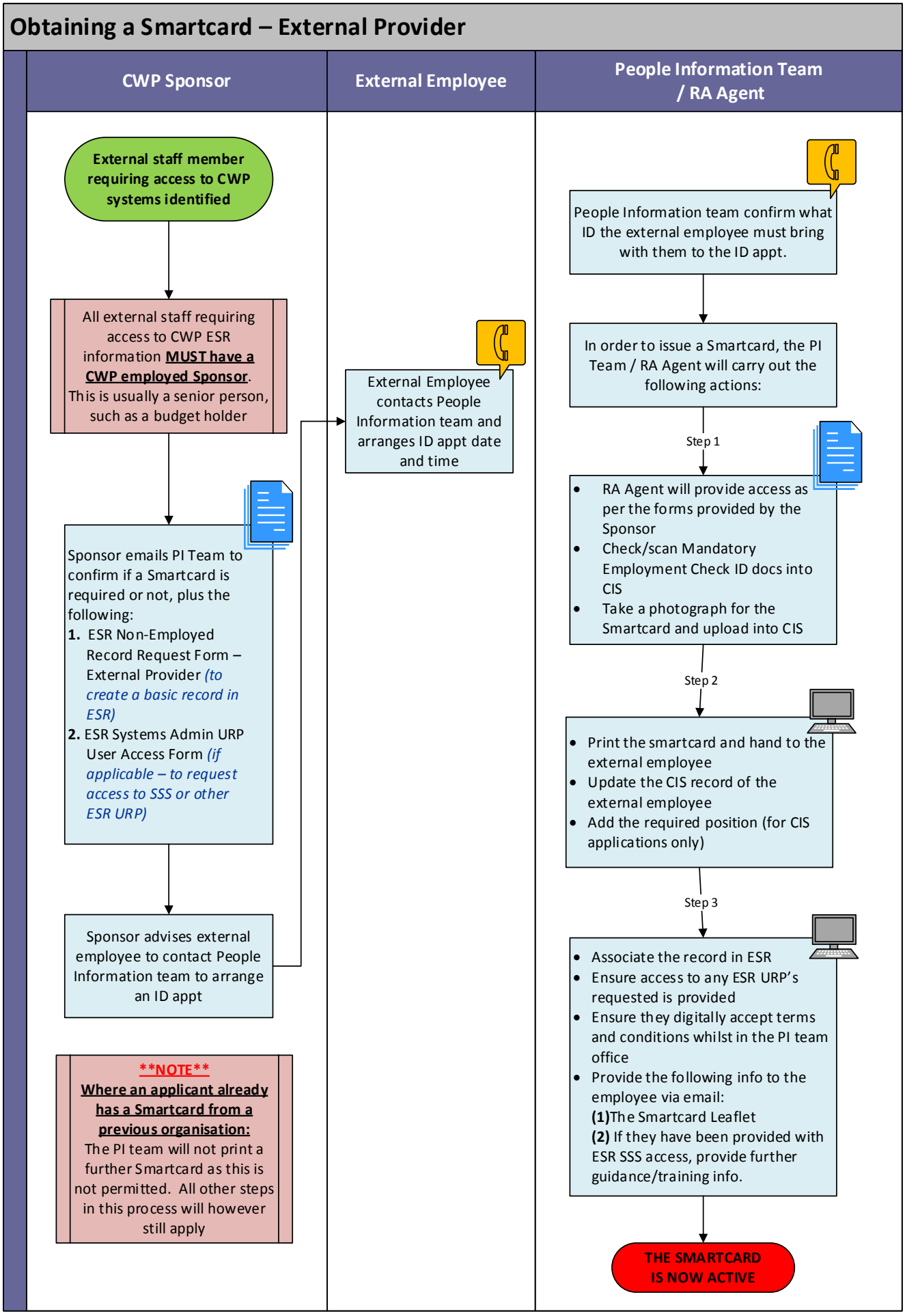
Do not retain a paper version of this document, always view from the website www.cwp.nhs.uk to ensure it is the correct version

6.13 Appendix 1 - Obtaining a Smartcard – New Starter



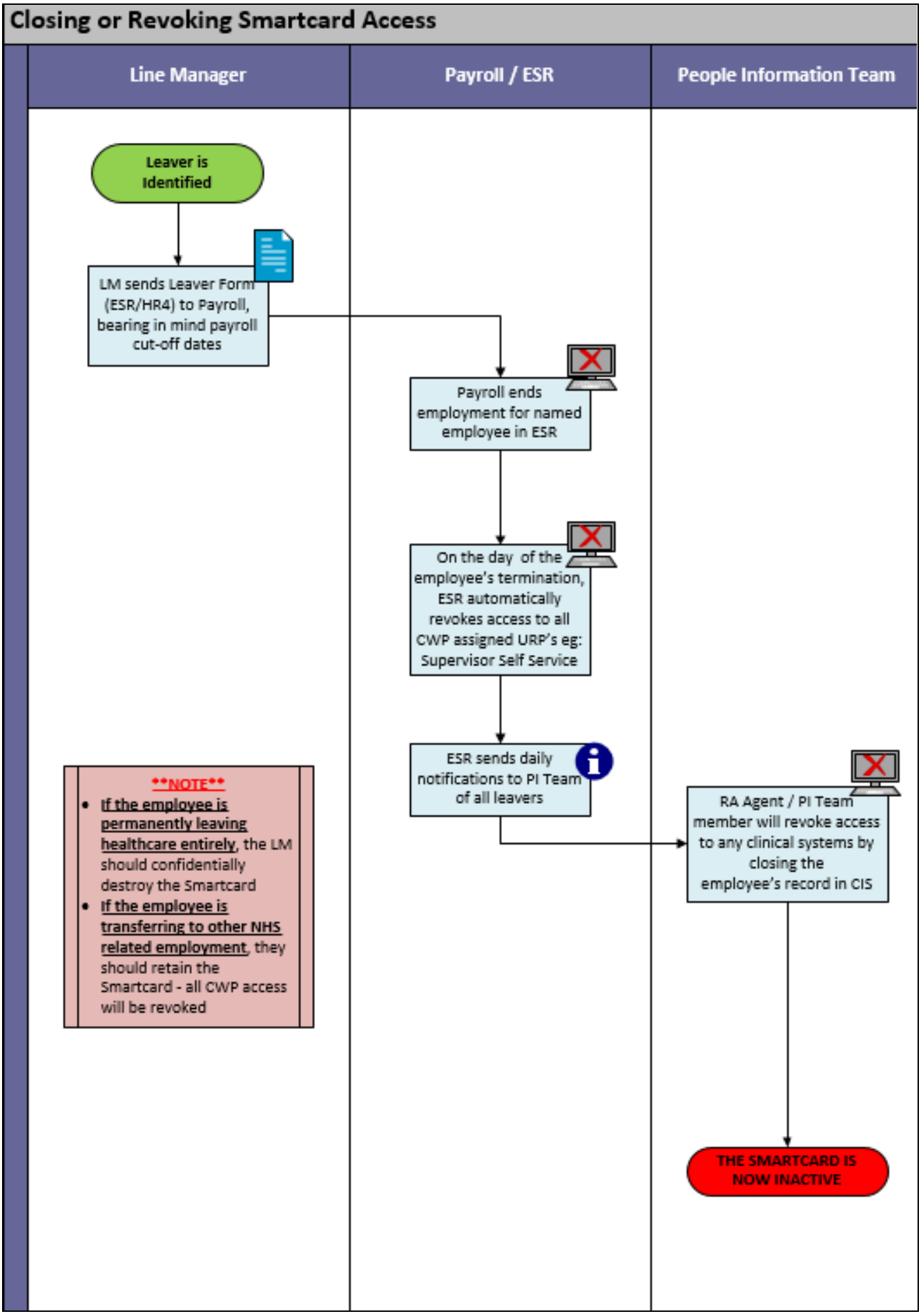
Do not retain a paper version of this document, always view from the website www.cwp.nhs.uk to ensure it is the correct version

Appendix 2 – Obtaining a Smartcard – External Provider



Do not retain a paper version of this document, always view from the website www.cwp.nhs.uk to ensure it is the correct version

Appendix 3 - Closing or Revoking Smartcard Access

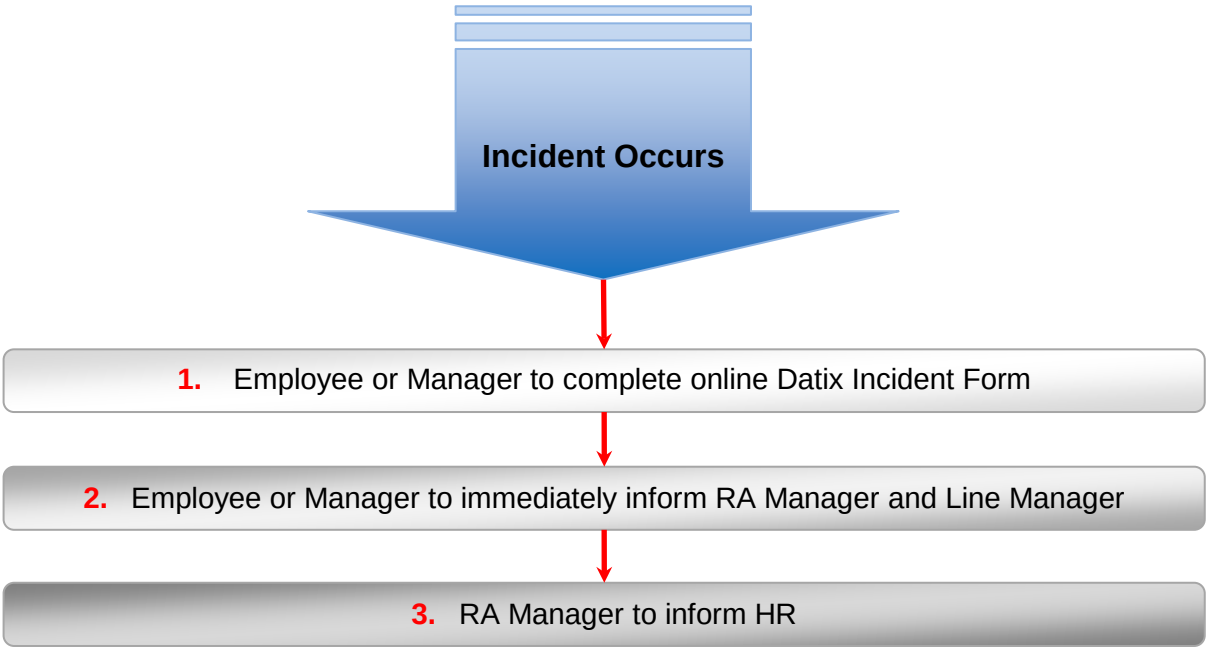


Do not retain a paper version of this document, always view from the website www.cwp.nhs.uk to ensure it is the correct version

6.16 Appendix 4 - Incident Grading Matrix

Adverse incidents should be classified according to seriousness of the outcome and in accordance with the following system:

Category	Definition	Actual or potential event consequence	Event detail / description
A Most severe	Unauthorised access to National Care Record applications	• Major breach of security and confidentiality. • Sponsor to report immediately to RA	• Investigate under CWP's Disciplinary Policy and Procedure.; • Possible disruption to carrying out role; • Severe loss of confidence in the process by staff and public; • Possible litigation for the Trust.
B Severe	Non-compliance of local or national policy	• Major breach of RA contract by not following correct process and procedures. • Sponsor to report to RA	• Investigate under CWP's Disciplinary Policy and Procedure.; • Possible disruption to carrying out role
C Medium Severity	Application Misuse	• Moderate disruption to process by wrongful use of smartcard or accessing programme with another smartcard. • Sponsor to report immediately to RA	• Investigate under CWP's Disciplinary Policy and Procedure.; • Possible service disruption
D Low Severity	Lost, stolen or damaged smartcard	• Moderate disruption to process. • Incident to be reported immediately to Sponsor	• Possible service disruption • Possible temporary disruption to carrying out role as unable to access without smartcard
E Low Severity	Forgotten Pin, blocked card	• Moderate disruption to process. • Incident to be reported to IT Servicedesk	• Possible service disruption • Possible temporary disruption to carrying out role as unable to access without PIN



Do not retain a paper version of this document, always view from the website www.cwp.nhs.uk to ensure it is the correct version