INTEGRATED IDENTITY MANAGEMENT (IIM) PROCESS POLICY

Department / Service:	Human Resources/ Knowledge Management	
Originator:	Kirstyn Lovegrove David Chamberlain Emma Gibbs	Head of Workforce Systems Library & Knowledge Services Library & Knowledge Services
Accountable Director:	Alison Koeltgen	Chief People Officer
Approved by:	Information Governance Steering Committee	
Date of approval:	24th March 2026	
Review Date: **This is the most current document & should be used until a revised version is in place**	24th March 2029	
Target Organisation(s)	Worcestershire Acute Hospitals NHS Trust	
Target Departments	Trust wide	
Target staff categories	Registration Authority (RA) staff; staff administering the workforce, recruitment, payroll & HR functions on ESR; Information Governance personnel, smartcard users & IT/Digital colleagues.	

Policy Overview

The purpose of the first edition of the policy was to outline the agreed working practices required to support the Electronic Staff Record (ESR) interface to the User Identity Manager (UIM) software used to provide the electronic management of access control.

In February 2015 UIM software was replaced by Care Identity Service (CIS) software which has led to some changes in procedure. A new national Registration Authority Policy was published in March 2019 which lays out the RA policy requirements that every organisation which has a Registration Authority needs to adhere to. A full operational & process guidance document was released in February 2016

This revision has taken the changes into account including the rebranding of CIS to Care Identity Management (CIM) & complies with the national policy & procedure. It is not intended to be an exhaustive review of all HR/RA processes & procedures but rather will focus on the key processes for creating NHS Care Identities as well as the issuance of both physical (Smartcards) & alternative authenticators (iPad fingerprint, Microsoft Authenticator, Windows Hello, Security key, NHS.net Connect, Passkey, Robotic Process Automation authenticator. This policy change also ensures that the name Registration Authority Manager has been updated in accordance with the national policy.

The policy will be of primary interest to those staff working within the Registration Authority (RA) function of the Trust & HR teams of ESR. It will also be of interest to managers requiring smartcards for their teams & IT/Digital & Information Governance personnel.

Key amendments:

Date	Amendment	By:
06/08/2015	Document extended for 12 months as per TMC paper approved on 22nd July 2015	TMC
14/11/16	Further extension as per TMC 22nd July 2015	TMC
December 2017	Document extended for 3 months as per TLG recommendation	TLG
March 2018	Document extended for 3 months as approved by TLG	TLG
June 2018	Document extended for 3 months as per TLG recommendation	TLG
February 2020	Document extended for 3 months whilst approval process is completed	David Chamberlain
May 2020	Document extended for 6 months during COVID-19 period	
22nd Jan 2021	Document extended for 6 months to enable thorough review to take place	David Chamberlain
11th June 2021	National RA policy link upgraded to 2020.	David Chamberlain
29th January 2025	Document extended for another 6 months whilst under review	David Chamberlain
3rd February 2026	Policy updated with modern terminology & links to the latest Registration Authority policy	Emma Gibbs

Contents **Page**

1 Introduction

1.1 From April 2008, NHS Employment Check Standards became a requirement in the NHS as part of the annual health check. Similarly, robust identity checks were also enforced using the same identity management standards carried out by an NHS organisation's Registration Authority (RA) to verify an individual's identity before allowing access to NHS Care Records Service (NHS CRS) applications. Details of the requirements are given in the NHS Employers publication *Identity checks* http://www.nhsemployers.org/your-workforce/recruit/employment-checks/nhs-employment-check-st&ards/identity-checks

Combining these two parallel activities into a single **Integrated Identity Management** (IIM) process has been shown to deliver significant benefits

through HR/RA process integration & the move to Position Based Access Control (PBAC).

1.2 ESR-CIM Interface is used to link staff records in ESR to user records in NHS CRS to remove duplication & to drive access control based on the job that a person holds. HR functions currently update ESR when changes are made regarding an employee's assignment to an established ESR position. Where this position is linked to an NHS CRS Access Control Position, the ESR interface will be triggered by such changes & will automatically update an individual's access rights to NHS CRS compliant systems to reflect the requirements of their new position or status.

1.3 The main benefits are:

- Efficiency savings
  - The achievement of a paperless system for smartcard registration
  - De-duplication of identity checks

- Improved governance
  - Automatic cancellation of NCRS access on leaving employment
  - Online signature of terms & conditions
  - Standard positions allocated for job roles through ESR

1.4 This policy document is compliant with the current Registration Authority Policy version 2.5 & Registration Authorities Operational & Process guidance.

2. Scope of the Policy

The policy applies to all employees & external contractors who require an authenticator associated with Worcestershire Acute Hospitals NHS Trust to access systems securely & as identified by their position.

2.1 It is particularly relevant for staff working within the Registration Authority (RA) function of the Trust & on the workforce, recruitment, payroll & HR functions of ESR. It will also be of interest to managers requiring smartcards for their teams & IT/Digital & Information Governance personnel.

2.2 The document is not intended to be an exhaustive review of all HR/RA processes & procedures but rather will focus on the key processes for issuing authenticators to allow access to NHS systems.

2.3 Currently, Worcestershire Acute Hospitals NHS Trust uses authenticators for access to the following systems:

- Care Identity Management
- ESR Manager/Supervisor Self Service
- ESR e-learning
- E-Referral Service (formerly Choose & Book)
- Child Protection Information System (CP-IS)
- Cervical Screening Management Service (CSMS)
- Bowel Cancer Screening Service (BCSS)

- Directory of Service
- Secondary Uses Service (SUS)
- Multi-Factor Authentication
- MESH

3 Definitions

Access Control Position (ACP)
An ACP contains a set of access rights that have been approved & granted though the RA process.

Care Identity Management (CIM)

Care Identity Management allows NHS & healthcare staff to be registered for a 'Care Identity' - a digital identity that can then be associated with health & care organisations they work for.

The system is used to assign & manage permissions that enable appropriate access to clinical systems & patient information. It is also used to assign authentication tokens that allow healthcare professionals to perform multi-factor authentication to these clinical & patient record systems.

The Good Practice Guide (GPG) 45
Good Practice Guide (GPG) 45 helps you decide how to check someone's identity.

Electronic Staff Record (ESR)
The electronic human resources management system used by most organisations within the NHS.

Integrated Identity Management (IIM)
IIM provides an interface for the separate ESR process maintained by the Workforce Transformation Team & the CIS process maintained by the RA Team for capturing & managing an employee's identity & access to the Care Identity Managed Systems.

NHS Care Records Service (NCRS or NHS CRS)
NCRS is a service that allows health & social care professionals to access & update a range of patient & safeguarding information across regional integrated care system (ICS) boundaries.
The service provides a summary of health & care information for care settings where the full patient record is not required to support their direct care. It is a web-based application & can be accessed regardless of what IT system an organisation is using.
The NCRS provides access to over 63 million patient records.

NHS Smartcard
A plastic card containing an electronic chip that is used to access the NCRS & other NHS IT applications, along with a passcode. The chip does not contain any personal information.

Alternative Authenicators

The RA Team can issue alternative authenticators as listed below should the system/services allow. **iPad** (Uses fingerprint biometrics on an iPad to authenticate), **Microsoft Authenticator** (Uses an approved email and security code to access National Care Records Service), **Windows Hello** (Uses facial recognition, fingerprint or PIN on supported Windows devices), **Security key** (Uses a small physical device that is a software free alternative to smartcards), **NHS.net Connect** (Uses an NHS.net Connect account to authenticate), **Passkey** (Uses secure technology on a device to allow authentication without a password), **Robotic Process Automation authenticator** (Automate a range of back-office and administrative functions to free up time) More information can be found Care Identity Service authenticators - NHS England Digital

Position Based Access Control (PBAC)

The PBAC concept groups access control requirements by job role allowing any number of employees to share generic access rights based on what they do rather than who they are. The positions can be associated with ESR positions thus enabling the inheritance of access rights via the ESR position that the employee is assigned to.

Registration Authority (RA)

The organisational structure within an NHS organisation that is responsible for registering & verifying the identity of health care professionals/workers who need access to the NHS Care Records Service or other NHS IT applications. Staff need to prove their identity & have their application approved by a sponsor (usually their line manager) before being issued with a smartcard by the RA. The RA grants them an approved level of access. This process is essential to protect the security & confidentiality of the systems. The Executive Management Team of the NHS organisation should embed governance of their RA in the information governance & performance management framework.

Role Based Access Control (RBAC)

A national standard set of job roles & related activities & areas of work which can be approved by a sponsor & granted by the RA to a user. The database & users guide are at National role-based access control (RBAC) for developers - NHS England Digital, the NHS digital national Role Based Access Code (RBAC) table can also be downloaded from that page.

User Identity Manager (UIM)

UIM was the registration software managing access control to NHS CRS systems before the introduction of CIS & now CIM.

User's Unique Identifier (UUID

The UUID is randomly applied on registration of users in CIM. It is displayed under the photo on the smartcard. The number is also held against employee records in ESR to validate that the employee has an active entry on NHS CRS.

4. Responsibility & Duties

In terms of Public Key Infrastructure (PKI) there is a single Registration Authority (NHS England). All organisations that run a local Registration Authority do so solely on a delegated authority basis from NHS England. As NHS England is the single Registration Authority it needs to assure itself that organisations are operating

appropriately & discharging their duties in an effective & consistent fashion described in the National RA Policy document.

The local Registration Authority consists of the Board level individual accountable for RA activity, RA Manager, RA Agents & sponsors (Line Managers) who have responsibility to individuals providing healthcare services to the NHS directly or indirectly to ensure timely access to spine-enabled applications in accordance with their healthcare role. The RA Managers are appointed by the Board or executive management team & have a written letter of appointment which they hold stored in a safe environment. It is recommended that there should be a minimum of two individuals assigned to the RA Manager role for business continuity reasons.

4.1 Directorate level

Overall responsibility for this policy rests with the Trust Board. The lead Executive Director will be the Chief People Officer who has responsibility for ensuring that:

- The policy is implemented & operated effectively
- An audit trail is maintained
- All staff involved with the administration of IIM are aware of the policy & the procedures that apply to them.
- The accountable Director must report annually to the board on RA activity in the Trust & must sign off the RA IG Toolkit submissions.

4.2 RA Manager

The Trust's RA Managers are responsible for running the governance of the RA for Worcestershire Acute Hospitals NHS Trust. This involves:

- Agreeing & signing off local operational processes.
- Ensuring that these processes are being adhered to.
- Registering RA staff.
- Ensuring the effective training of RA staff.
- Facilitating the process for agreeing to the organisation's access control positions.
- Ensuring that appropriate auditing is carried out.
- Ensuring users are compliant with the terms & conditions of smartcard usage.
- Ensuring verification of user's ID is in line with Good Practice Guide 45 – How to prove & verify someone's identity
- Ensuring leavers have their access rights removed in a timely manner.
- Ensuring the security of RA records including archived paper records which must be kept for a period of either 6 years after the subject leaves service or until the subject's 79th birthday whichever is the later.
- Ensuring all service issues are raised appropriately locally & nationally.

4.3 Trust Sponsor/Line Managers

Line managers are responsible for informing the RA Manager via the New Starter form or the Smart Card Request form of appropriate personal details for members of staff who require smartcard access in the course of their duties. It is expected that they will be able to give an indication of the access requirements.

In case of a variance between the role requested by the line manager & that allocated by the Trust Sponsor, the RA Manager will consult with both parties to

resolve the matter.

4.4 RA Agent Advanced

The CIM system introduced an additional level of authority. Advanced RA Agents can perform nearly all the RA processes available to the RA Manager except for assigning users to their RA roles.

4.5 RA Agent

An RA agent can check ID, register smartcard users, unlock smartcards & renew certificates.

4.6 RA Agent – ID Checker

This role checks the user's identity at the pre-employment stage for new starters either within the Recruitment Team or Medical Resourcing. They enter the ID documents seen into the ESR system for the RA Agents to process the smart card request.

4.7 Local Smartcard Administrator

This role can only unlock smartcards & assist in the renewal of certificates. The role is not currently allocated in Worcestershire Acute Hospitals NHS Trust.

4.8 Trust employees

Those employees who are deemed by their line manager to require a smartcard must:

- Provide the correct identity documents as defined in the Good Practice Guide 45 – How to prove & verify someone's identity
- Undertake to observe the agreed terms & conditions & electronically sign this declaration when their card is issued (Appendix C).

4.9 External contractors

External contractors to the Trust who require access to systems accessed by smartcard will need to abide by the same terms & conditions as employees. Their application must be sponsored by a senior manager employed by the Trust. Their smartcard access will be set to expire on the end date of their contract. If the end date is not known, it will be set at 3 months from the start date.

5 Creation of a national digital identity

All users, including RA staff, must have only one NHS smartcard issued to them showing their UUID & photograph. The primary purpose of NHS smartcards is to provide identification & system authentication to spine-enabled applications.

5.1 Identity verification

Identity must be verified in a face-to-face meeting either at the pre-employment stage for new starters by the Recruitment Team or Medical Resourcing. They enter the ID documents seen into the ESR system for the RA Agents to process the smart card request. Or by an RA Agent if the staff member does not have any ID listed in their ESR Record. ID checks will also need to be completed for any contractors or locums that sit outside of the ESR system. It must be done by

examining original documents & seeing that the identity relates to the individual who presents themselves at the meeting. This provides assurance that the identity is valid across any organisation an individual works within. ID Checks must comply with the Good Practice Guide (GPG) 45

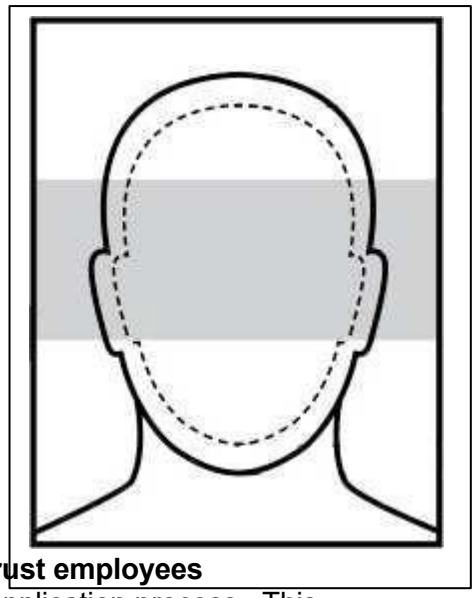
The documents that can be used to verify an identity are listed in the NHS Employers publication *Identity checks* which can be currently found at http://www.nhsemployers.org/your-workforce/recruit/employment-checks/nhs-employment-check-st&ards/identity-checks

5.2 Photographs

The photograph assigned to the user's profile & printed on the smartcard must adhere to the following standards & specifications:

- It must be cropped so that it appears as in the diagram.
- It must be taken against a plain background with adequate lighting.
- On completion of the registration process the photograph should be removed from local files as it is then stored securely on CIM.

Further information is at Get a passport photo: Digital photos - GOV.UK



6. Registration processes

6.1 Process for Worcestershire Acute Hospitals NHS Trust employees

All staff requiring a smart card need to go through the application process. This is by completing a smart card request form or section of the new starter electronic form. This form with or without a photograph gets emailed to the generic smart card email address. An RA Agent will process the application by entering the details onto the relevant spreadsheet according to the employee's work base. The form & picture are saved on the shared drive with the picture being deleted after use. The form is retained according to national guidance. A search against the ESR Mandatory Employment Checks is completed to see if there are any Identification Documents listed against the employee record (by recruitment or medical resourcing). If the ID Documents are present, then the application can move onto the next stage of association. If not, the applicant is invited in to have a photograph taken & ID check completed by RA staff in accordance with the Good Practice Guide (GPG) 45 & recorded on the spreadsheet accordingly with the photograph being saved on the shared drive.

Once the ID has been recorded & entered against the employees record in ESR the RA Agent can perform a search on the ESR RA Workbench. The purpose of this search is to either create the link to CIM & Worcestershire Acute Hospitals NHS Trust (association) or to generate a request to create a Care Identity on CIM. If the employee has previously had a Care Identity created this will show up in the search & an association can be created, if not then the option to create a Care Identity is given.

Once the association or creation has been requested a check is needed on the CIM system to approve the request or to complete the creation of the Care Identity.

For associations the approval is only needed should any personal details have changed from the current details on CIM to those being pulled through from ESR.

For creations, demographic information is pulled through from ESR, but the picture will need to be imported from the shared drive, once the Care Identity is created the search on the ESR Workbench is done again & this time the association is made.

If the user has previously had a Care Identity, & they have a valid & up to date smart card (check completed on CIM) an association email is sent to the user. If there is no smart card listed or if it is an outdated version of a smart card, the process to print a card is initiated at this stage. The spreadsheet is updated at this stage.

For those who have just had a new Care Identity created a smart card needs to be printed. Once the card is printed the spreadsheet is updated with the relevant information & the user is emailed to collect their card. The photograph is deleted from the shared drive & the spreadsheet updated to confirm this action has been done.

6.1.1 New starters with smartcards issued by other Trusts

New starters are now managed via the New Starter Electronic form. Within this form there are sections relating to smart cards. If a new member of staff is required by their recruiting manager to have a smartcard the recruiting manager completes the relevant section and then the new staff member answers questions relating to whether they have had card previously & if so asks them for the card details. The new staff member includes a passport-style photograph, & this is verified by the recruiting manager as a true likeness. Once the form is completed, the relevant section is emailed to the generic smart card mailbox for processing. The process is the same as above in section 6.1.

6.1.2 Personal details changes

The ESR system automatically informs the RA via request in CIM of any personal detail changes, ensuring that the data is kept up to date in CIM & consistent with ESR. Once a name change appears on CIM then the RA Team send the staff member an email asking them to arrange an appointment with an RA Agent to arrange for the name change document to be seen & a new smartcard printed.

The personal details that are synchronised between ESR & CIM are as follows:

Title
Surname
First Name
Middle name
NI Number
Date of Birth
Email address

Work phone number
Work mobile number

If a change in core identity is requested such as a change of name, appropriate proof such as a marriage certificate must be seen.

6.1.3 External Shared Services Staff

External shared services staff include members of staff not directly employed by the Trust who assist in various elements of ESR including payroll, bulk updates of data & transfer of staff.

As these staff are not assigned to an ESR position they cannot have their NHS Care Identity access for Worcestershire Acute Hospitals NHS Trust controlled using the ESR-CIM Interface. However, they still require their Smartcard UUID to be entered into ESR to ensure that they can use their Smartcard to access the Trust's virtual private databases.

This requires ID checks to be recorded in ESR for the user & the 'association' to be completed using the RA Workbench rather than the ESR record.

6.2 CIM-only processes

CIM is used without connecting to ESR for managing NHS CRS System access for non-employees. These can be contractors (eg Health Records staff employed by Xerox) or employees of other NHS Trusts (eg Herefordshire & Worcestershire Health & Care NHS Trust staff who require access to Trust systems such as the E- Referral Service).

6.2.1 Contractors

The contractor's line manager within Worcestershire Acute Hospitals NHS Trust will complete a smart card request form in the usual manner. Ensuring all the mandatory data is completed including their contracted end date. The request will also be recorded on the appropriate spreadsheet, & an appointment agreed with the new starter who will attend a face-to-face meeting with the RA staff & produce their ID documentation.

The RA Staff will then verify the person's ID & enter the relevant information into the spreadsheet & take a photograph of the user. RA staff will then add the details in CIM & print & issue the card, with the user electronically signing the terms & conditions. The card will be set to expire at the end date of the contract, or in 3 months if there is any doubt.

6.2.2. Inter-organisational agreements

Currently we have arrangements in place with Herefordshire & Worcestershire Health & Care NHS Trust & our staff members who need access to the Oncology System called SystmOne which is managed by Herefordshire & Worcestershire Health & Care NHS Trust, we request the access via their RA Team. Access is provided to our staff via the CIM system & is in place for 12 months. Herefordshire & Worcestershire Health & Care NHS Trust staff who need to book patients into Worcestershire Acute NHS Trust hospitals using the e-referral service are again provided with relevant access for 12 months, the requests are emailed in from the Herefordshire & Worcestershire Health & Care NHS Trust RA Team & we add access for 12 months.

6.3 Temporary access cards (TACs)

Temporary access cards (TAC) are available for staff across all areas of our organisation. TAC cards can only be used by users who have already verified their identity and have a national care identity on CIM. TAC cards do not have any positions assigned to them until the need arises & the appropriate access is assigned for an agreed short period of time.

Worcestershire Acute Hospitals NHS Trust has decided that temporary access cards are only issued by RA staff in the following circumstances:

- The user does not have their smartcard with them; they need to use it immediately & it is not feasible to collect it.
- The user needs different or continued access & RA functionality is not available to do this.

6.3.1 Creating a TAC

TAC profiles are created in accordance with national guidance as found here - Create a new Temporary Access Card (TAC) profile - NHS Engl& Digital.

6.3.2 Issuing a TAC

RA staff verify that the individual has a national care identity & check that the photograph on their record is a true likeness.

A manual issue log is maintained for each TAC containing the following information: smartcard TAC name & UUID; reason for issue; time & date of issue; name & UUID of RA staff member issuing TAC; return time & date.

A TAC should normally be issued for a maximum of 72 hours.

On return, the TAC should be locked by entering an incorrect passcode 3 times.

The RA Manager will monitor the use of TACs & the issue log on a regular basis.

7. Positions Setup & Maintenance

7.1 Position Based Access Control (PBAC)

Worcestershire Acute Hospitals NHS Trust positions are managed within CIM and are linked to the appropriate positions within ESR. These positions are reviewed annually with Workforce and Information Governance. Any new positions are agreed with Information Governance and Workforce and created by the RA Manager in accordance with the instructions here Create a new position - NHS England Digital.

7.2 Changes to Access Control Positions

Any changes to positions will need to be approved by the Information Governance Steering Group, or if urgent, by the Information Governance Manager, before the amendments are made.

8. Implementation & dissemination

The revised policy has been updated to include new terminologies and updated links. The policy will go on the Key Documents website, Smartcard intranet pages and will publicised through the Trust /Library newsletters.

9. Training

9.1 RA Staff

The RA Manager ensures all RA staff have completed the e-learning provided by here National Registration Authority and Smartcard Policy - elearning for healthcare.

The RA Manager will attend all relevant IAM Roadshows/Feature focuses and if the RA Agents are not able to attend will cascade accordingly.

9.2 Users

New smartcard users are prompted on the first login to sign and abide by the terms and conditions of use.

If required, the RA Agent will provide an introductory session on how the smart card works and how to perform some of the self service options as well as how to keep in touch with the RA Team.

10. Monitoring & Compliance

Reports can be run from the CIM system to provide accurate data collection. However, our local spreadsheets also provide invaluable information that will be continued. R eports will be submitted to the Trust's Information Governance Steering Group on a quarterly basis.

The full audit policy is given at Appendix D.

11. Policy Review

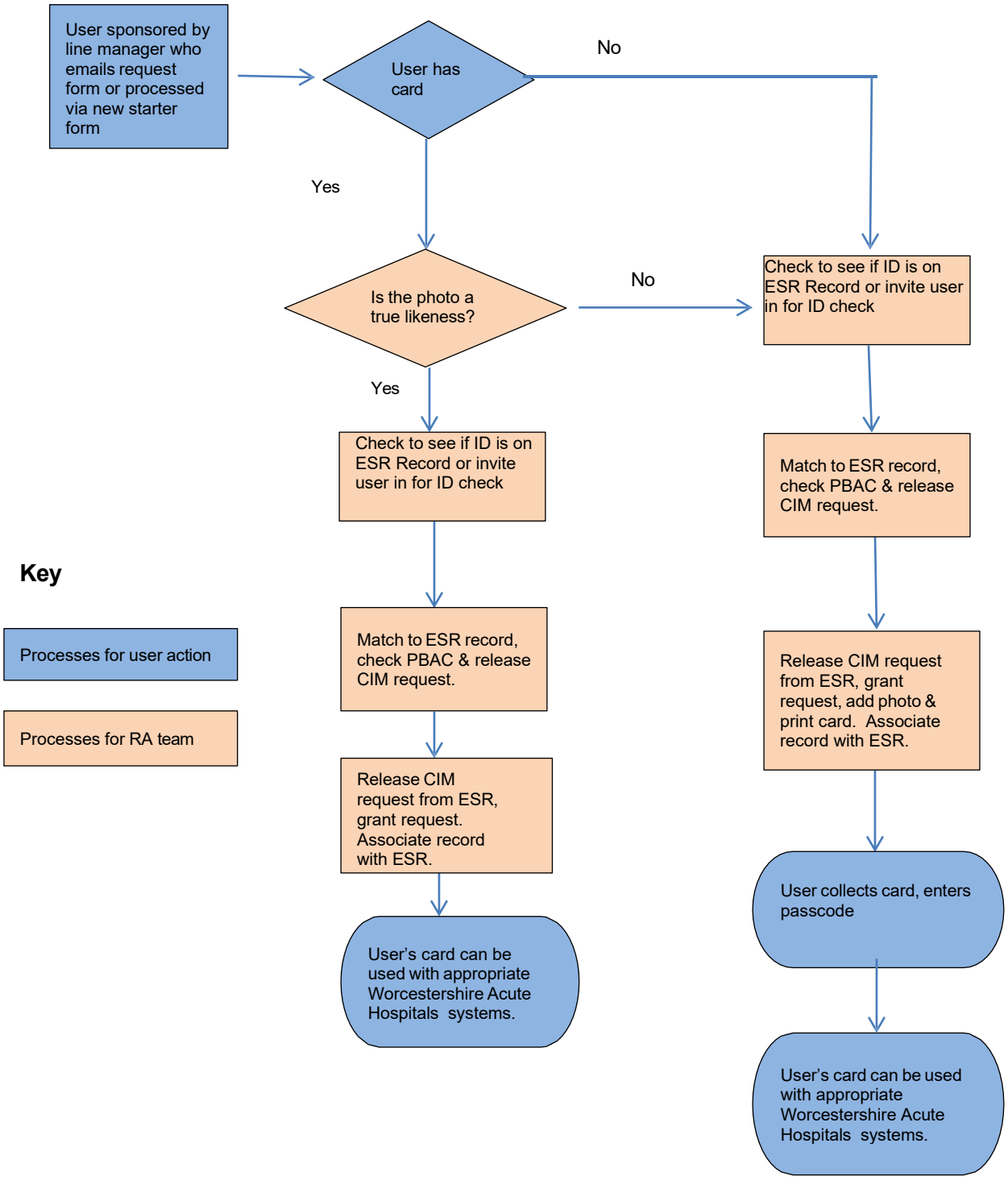
The Information Governance Strategy Group will review this policy on a biennial basis, or more frequently if required.

12. References

Document	URL
Registration Authority Policy NHS Digital, Updated online July 2024.	Registration Authority policy - NHS England Digital
Registration Authorities Operational & Process Guidance 2016.	Registration Authorities Operational & Process guidance.
Identity checks. NHS Employers, Updated online June 2025.	http://www.nhsemployers.org/your-workforce/recruit/employment-checks/nhs-employment-check-st&ards/identity- checks
Registration Authorities training modules	National Registration Authority and Smartcard Policy - elearning for healthcare.
Data Security & Protection Toolkit Updated January 2026	Data Security and Protection Toolkit

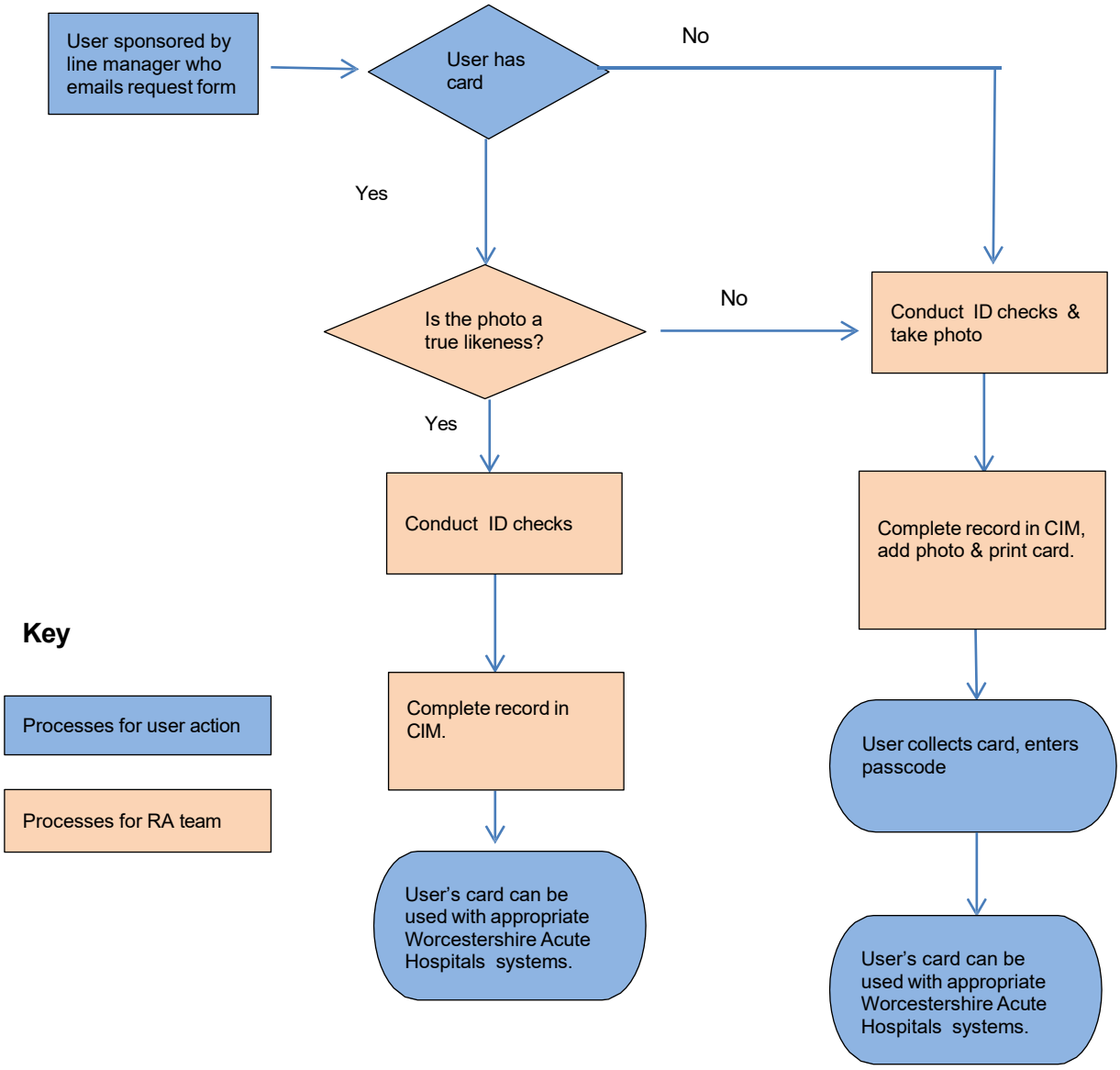
Appendix A:

Registration Process for Worcestershire Acute Hospitals Employee



Appendix B:

Registration Process for External Users



Appendix C NCRS Smartcard User Terms & Conditions

Terms for using our service

By using our service, you, the applicant, confirm the following:

1. You understand and accept that your personal data will be used by us as described in the privacy notice for users of CIS2 and CIS. Each user must have their identity assured and verified to the relevant standard applicable at the time of registration. This is currently Good Practice Guide GPG45 (or recognised successor) on the identity proofing and verification of an individual to a minimum of Level 3. In specific circumstances, we may allow an individual to create a lower level identity with limited access to limited systems. This requirement may be refreshed from time to time.
2. You confirm that the information which you provide in the process of your application is complete, true and accurate. You agree to notify your local Registration Authority immediately of any changes to this information.
3. You understand and accept that the Authentication Token (with the exception of personally owned devices which you provide) issued to you is the property of / licensed to the health and social care bodies providing it to you. You agree to use the Authentication Token to access NHS Spine and other CIS2 approved applications only in the normal course of your employment or contract arrangement.
4. If you wish to use Apply for Care ID you must have an internet connection and an appropriate device for access, like a smartphone. We do not guarantee that Apply for Care ID will always be available, or that access to it will be error free.
5. We may suspend, stop, remove, update or change CIS, CIM, CIS2 or Apply for Care ID without notice at any time.
6. You agree that you will check the operation of your Authentication Token promptly after you receive it. This will ensure that you have been granted the correct access profiles. You also agree to notify your local Registration Authority promptly if you become aware of any problem with your Authentication Token or your access profiles.
7. You understand that the suppliers of some Authentication Tokens may process personal data about you as an independent Controller and may have applicable privacy policies and terms and conditions. You will be presented with these as part of download/registration and are responsible for reviewing and abiding by these.
8. You agree that you will keep your Authentication Token private and secure and that you will not permit anybody else to use it or to establish any session with the NHS Spine applications. You will not share your passcode with any other user. You will not write your passcode down, nor use any kind of electronic storage (media or otherwise) to store it, for example by using a programmable function key on a keyboard. You will take all reasonable steps to ensure that you always leave your workstation secure when you are not using it by removing your Physical Smartcard or locking your Authorised Device or iPad Device. If you lose your Authentication Token or if you suspect that your Authentication Token has been stolen or used by a third party, you will report this to your local Registration Authority as soon as possible.
9. You agree that you will only access the NHS Spine application by using an Authentication Token approved by NHS England, as part of the CIS2 registration process. You agree that your use of the Authentication Token, the NHS Spine applications and all patient data shall be in accordance with the NHS Confidentiality Code of Practice and (where applicable) in accordance with your contract of employment or contract of provision for service (whichever is appropriate) and with any instructions relating to the NHS Spine applications which are notified to you.
10. In respect of each service or product accessible through NHS Spine you agree that you will follow any instructions or conditions for use provided in respect of such service or product.
11. You agree not to maliciously alter, neutralise, circumvent, tamper with or manipulate your Authentication Token, NHS Spine applications components, the Apply for Care ID service or any access profiles given to you.
12. You agree not to deliberately corrupt, invalidate, deface, damage or otherwise misuse any NHS Spine applications or information stored by them or the Apply for Care ID service. This includes, but is not

limited to, the introduction of computer viruses or other malicious software that may cause disruption to the services or breaches in confidentiality.

13. You acknowledge that your access may be audited. You understand and accept that your Authentication Token may be revoked, or your access profiles changed at any time without notice if you breach these terms and conditions; if you breach any guidance or instructions notified to you for the use of the NHS Spine applications or if such revocation or change is necessary as a security precaution. You also understand and accept that if you breach these terms and conditions this may be brought to the attention of your employer (or governing body in relation to independent contractors) who may then take appropriate action (including disciplinary proceedings and/or criminal prosecution).
14. You understand and accept that the Registration Authority's sole responsibility is for the administration of access profiles and the issue of Authentication Token for the NHS Spine applications. The Registration Authority is not responsible for the availability of CIS, CIM, CIS2, the NHS Spine applications or applications which use NHS Spine authentication or the accuracy of any patient data.
15. You understand and accept that you, or your employer, shall notify your local Registration Authority at any time should either wish to terminate these terms and conditions and to have your Authentication Token revoked e.g. on cessation of your employment or contractual arrangement with health care organisations or other relevant change in your job role.
16. We own or have the right to use all intellectual property rights ("NHS IPR") used for the provision of CIS, CIM, CIS2 and Apply for Care ID. This includes rights in copyright, patents, database rights, trademarks and other intellectual property rights. You have permission to use CIS, CIM, CIS2 and Apply for Care ID for the sole purposes described in these terms and conditions. You need written permission from us or any other owner of NHS IPR to use these items in any other way.
17. Unless permitted by law or under these terms and conditions, you will:

- not copy CIS, CIM, CIS2 or Apply for Care ID except where such copying is incidental to normal use
- not rent, lease, sub-license, loan, translate, merge, adapt, vary or modify CIS, CIM, CIS2 or Apply for Care ID
- not combine or incorporate CIS, CIM, CIS2 or Apply for Care ID with any other programs or services
- not disassemble, decompile, reverse-engineer or create derivative works based on any part of CIS, CIM, CIS2 or Apply for Care ID
- comply with all technology control or export laws that apply to the technology used by CIS, CIM, CIS2 or Apply for Care ID

18. You understand and accept that we may unilaterally change CIS, CIM, CIS2, Apply for Care ID and these terms and conditions from time to time, and unless otherwise stated such changes will be effective immediately they become available. The latest version of these terms and conditions will be accessible during the authentication process and on our website. If we make any material changes to these terms and conditions we will inform you through your CIS2 / CIS account and will also send an email notification to all RA managers.
19. Although we make reasonable efforts to provide, maintain and update a robust CIS, CIM, CIS2 and Apply for Care ID service, they are provided 'as is'. To the extent allowed by law we make no expressed or implied representations, warranties or guarantees that your access to, or use of, CIS, CIM, CIS2 or Apply for Care ID will be unbroken or completely secure.
20. We will not be liable or responsible for any loss or damage caused by a virus, denial of service attack or any other harmful material that may infect your device, equipment, programs, data or other proprietary material due to your use of CIS, CIM, CIS2 or Apply for Care ID.
21. Nothing in these terms and conditions excludes or limits our liability for i) death or personal injury as a result of our negligence, ii) fraud or fraudulent misrepresentation or iii) any other liability which cannot be excluded or limited under English law.
22. Subject to the previous paragraph we will not be liable or responsible for any:

- loss or damage not caused by our breach of these terms and conditions
- business loss
- loss or damage arising from an inability to access or use CIS, CIM, CIS2 or Apply for Care ID

- indirect or subsequent losses that were not foreseeable to both you and us when you started using CIS, CIM, CIS2 or Apply for Care ID

23. Business loss includes loss of profits, revenue, contracts, savings, data, goodwill and wasted expenditure. Loss or damages are ‘foreseeable’ when they are an obvious result of our breach of these terms and conditions. Loss or damages are also 'foreseeable' if they were considered by you and us when you began using CIS, CIM, CIS2 or Apply for Care ID.
24. Each of the sections within these terms and conditions operate separately. If any section is invalid or unenforceable pursuant to applicable law, it will be superseded by a valid and enforceable provision that most closely matches the intent of the original. This includes warranty disclaimers and exclusions, and limits of liability. The remainder of these terms and conditions shall continue in effect.
25. If we delay in enforcing these terms and conditions, we can still enforce them later. If we do not insist right away that you follow the requirements within these terms and conditions, or we delay in taking steps against you if you break them, this will not prevent us from taking steps against you or prevent your need to follow the requirements at a later date.
26. You understand and accept that these terms and conditions form a binding agreement between yourself and all Registration Authorities who provide Registration Authority services to you. Non-compliance may also be treated as a disciplinary matter by your employer.
27. You understand and accept that these terms and conditions are governed by English law and that the English courts shall settle any dispute under these terms and conditions.

Last edited: 11 September 2025 9:33 am

Appendix D Governance

The mandatory governance requirements for organisations undertaking RA activities are as follows:

- The organisation must have a Board/EMT level individual who has overall accountability for the RA activity.
- This individual must report annually to the organisation on the RA activity.
- RA Managers are appointed by the Board/EMT. This appointment must be confirmed in an official document, such as minutes or a letter/email of appointment from the SRO.
- Every individual appointed to these positions must have a copy of the appointment evidence and make it available for inspection if asked.
- RA Managers are accountable for the running of RA activity in their organisation. They must set up systems and processes that ensure the policy requirements in this document are met.
- Any local processes must meet these policy requirements. Where catering for local organisation circumstances, these circumstances must not contradict the requirements set out in this document.
- RA Managers and Agents must keep up to date with national policy requirements, initiatives and changes. It is therefore mandatory to record their email address as part of their nationally verified digital identity.
- The Registration Authority and, where different, employing organisation must:
    - Have sufficient governance, processes and oversight in place to comply with Data Protection Laws. This includes, but is not limited to, providing fair processing information to all users. The RA should also ensure compliance with the NHS Code of Practice on confidential information and the Care Record Guarantee.
    - Be registered for the Data Security and Protection Toolkit and have a current latest status rating of 'standards met' as a minimum

Note that RA Managers are accountable to NHSE for upholding good RA practice in their organisation.

Supporting Document 1 - Equality Impact Assessment Tool

Equality and Health Inequalities Impact Assessment (EHIA) Tool

Herefordshire & Worcestershire STP - Equality and Health Inequalities Impact Assessment (HEIA) Form
Please read HEIA guidelines when completing this form

Section 1 - Name of Organisation (please tick)

Herefordshire & Worcestershire STP		Herefordshire Council		Herefordshire CCG	
Worcestershire Acute Hospitals NHS Trust	x	Worcestershire County Council		Worcestershire CCGs	
Worcestershire Health & Care NHS Trust		Wye Valley NHS Trust		Other (please state)	

Name of Lead for Activity	**David Chamberlain**

Details of individuals completing this assessment	**Name**	**Job title**	**e-mail contact**
	Emma Gibbs	**Digital Librarian/RA Manager**	**emmagibbs@nhs.net**
Date assessment completed	**03/02/2026**		

Section 2

Activity being assessed (e.g. policy/procedure, document, service redesign, policy, strategy etc.)	**Title:** INTEGRATED IDENTITY MANAGEMENT (IIM) PROCESS POLICY			
What is the aim, purpose &/or intended outcomes of this Activity?	To review policy & procedure to ensure it follows NHS Digital guidelines			
Who will be affected by the development & implementation of this activity?	X x	Service User Patient Carers Visitors	x ❑ ❑ ❑	Staff Communities Other _____

Is this:	x Review of an existing activity ❑ New activity ❑ Planning to withdraw or reduce a service, activity or presence?
What information & evidence have you reviewed to help inform this assessment? (Please name sources, eg demographic information for patients / services / staff groups affected, complaints etc.	NHS Digital website for Registration Authority
Summary of engagement or consultation undertaken (e.g. who & how have you engaged with, or why do you believe this is not required)	Updated links that were failing
Summary of relevant findings	Policy is now current

Section 3

Please consider the potential impact of this activity (during development & implementation) on each of the equality groups outlined below. **Please tick one or more impact box below for each Equality Group & explain your rationale**. Please note it is possible for the potential impact to be both positive & negative within the same equality group & this should be recorded. Remember to consider the impact on e.g. staff, public, patients, carers etc. in these equality groups.

Equality Group	Potential positive impact	Potential neutral impact	Potential negative impact	Please explain your reasons for any potential positive, neutral or negative impact identified
Age		x		Policy relates to access to system via clinical role & is neutral to this impact
Disability		x		As above
Gender Reassignment		x		As above
Marriage & Civil Partnerships		x		As above
Pregnancy & Maternity		x		As above
Race including Traveling Communities		x		As above

Religion & Belief		x		As above
Sex		x		As above
Sexual Orientation		x		As above
Other Vulnerable & Disadvantaged Groups (e.g. carers; care leavers; homeless; Social/Economic deprivation, travelling communities etc.)		x		As above
Health Inequalities (any preventable, unfair & unjust differences in health status between groups, populations or individuals that arise from the unequal distribution of social, environmental & economic conditions within societies)		x		As above

Section 4

What actions will you take to mitigate any potential negative impacts?	Risk identified	Actions required to reduce / eliminate negative impact	Who will lead on the action?	Timeframe
	Policy outdated	*Review Policy*	**RA Manager**	**2028**
How will you monitor these actions?	**RA Manager to put review date in calendar**			
When will you review this EIA? (e.g in a service redesign, this EIA should be revisited regularly throughout the design & implementation)	**March 2028**			

Section 5 - Please read & agree to the following Equality Statement

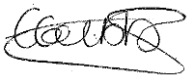
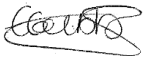
1. Equality Statement

1.1. All public bodies have a statutory duty under the Equality Act 2010 to set out arrangements to assess & consult on how their policies & functions impact on

the 9 protected characteristics: Age; Disability; Gender Reassignment; Marriage & Civil Partnership; Pregnancy & Maternity; Race; Religion & Belief; Sex; Sexual Orientation

1.1. Our Organisations will challenge discrimination, promote equality, respect human rights, & aims to design & implement services, policies & measures that meet the diverse needs of our service, & population, ensuring that none are placed at a disadvantage over others.

1.2. All staff are expected to deliver services & provide services & care in a manner which respects the individuality of service users, patients, carer's etc, & as such treat them & members of the workforce respectfully, paying due regard to the 9 protected characteristics.

Signature of person completing EIA	Emma Gibbs
Date signed	
Comments:	
Signature of person the Leader Person for this activity	
Date signed	03/02/2026
Comments:	

NHS Worcestershire Acute Hospitals NHS Trust

NHS Herefordshire and Worcestershire Health and Care NHS Trust

NHS Wye Valley NHS Trust

Herefordshire General Practice Taurus Healthcare

worcestershire county council

Herefordshire Council

Supporting Document 2 – Financial Impact Assessment

To be completed by the key document author & attached to key document when submitted to the appropriate committee for consideration & approval.

	Title of document:	Yes/No
1.	Does the implementation of this document require any additional Capital resources	No
2.	Does the implementation of this document require additional revenue	No
3.	Does the implementation of this document require additional manpower	No
4.	Does the implementation of this document release any manpower costs through a change in practice	No
5.	Are there additional staff training costs associated with implementing this document which cannot be delivered through current training programmes or allocated training times for staff	No
	Other comments:	

If the response to any of the above is yes, please complete a business case & which is signed by your Finance Manager & Directorate Manager for consideration by the Accountable Director before progressing to the relevant committee for approval