Public - To be published on the Trust external website

Title: Electronic Staff Record (ESR) Procedure

Ref: IT–0031-003-v3

Status: Approved
Document type: Procedure

Contents

1 Introduction

The following procedure document provides regulations and guidance for the management, security, and use of the Electronic Staff Record (ESR) system.

ESR is a national, integrated workforce management system. Staff information is not shared between Trusts and is only viewable within the individual organisation that the staff member works.

ESR provides information to support the Trusts business activities, ensuring timely and accurate payment of staff salaries. Managers can update staff information via the use of the self-service functionality.

The ESR system interfaces with the following systems that are used at TEWV.

- Oracle Financials
- Bankers Automated Clearing Services (BACS)
- NHS Jobs
- Pensions Agency
- HM Revenue and Customs (HMRC)
- General Medical Council (GMC)
- Nursing and Midwifery Council (NMC)
- E-Rostering (Allocate)
- Integrated Information Centre
- Active Directory
- Intrepid (North East Deanery)

This procedure supports our Journey to Changes as set out in the overarching Access to Information Systems Policy.

2 Purpose

This document provides regulations and guidance for the specific access, security, and use of the Electronic Staff Record (ESR) System in use within Tees, Esk and Wear Valleys NHS Foundation Trust. Misuse of ESR can compromise the Trust's confidential information, staff information and otherwise adversely affect the Trust's interests and reputation.

This procedure when implemented should reflect anti-discriminatory practice. Any services, interventions or actions must take into account any needs arising from race, gender, age, religion and belief, communication, sensory impairment, disability and sexuality.

Please note there are some services within the Trust that use alternative electronic systems. This document only relates to the use of ESR.

3 Who this procedure applies to

This procedure applies to all users of the system.

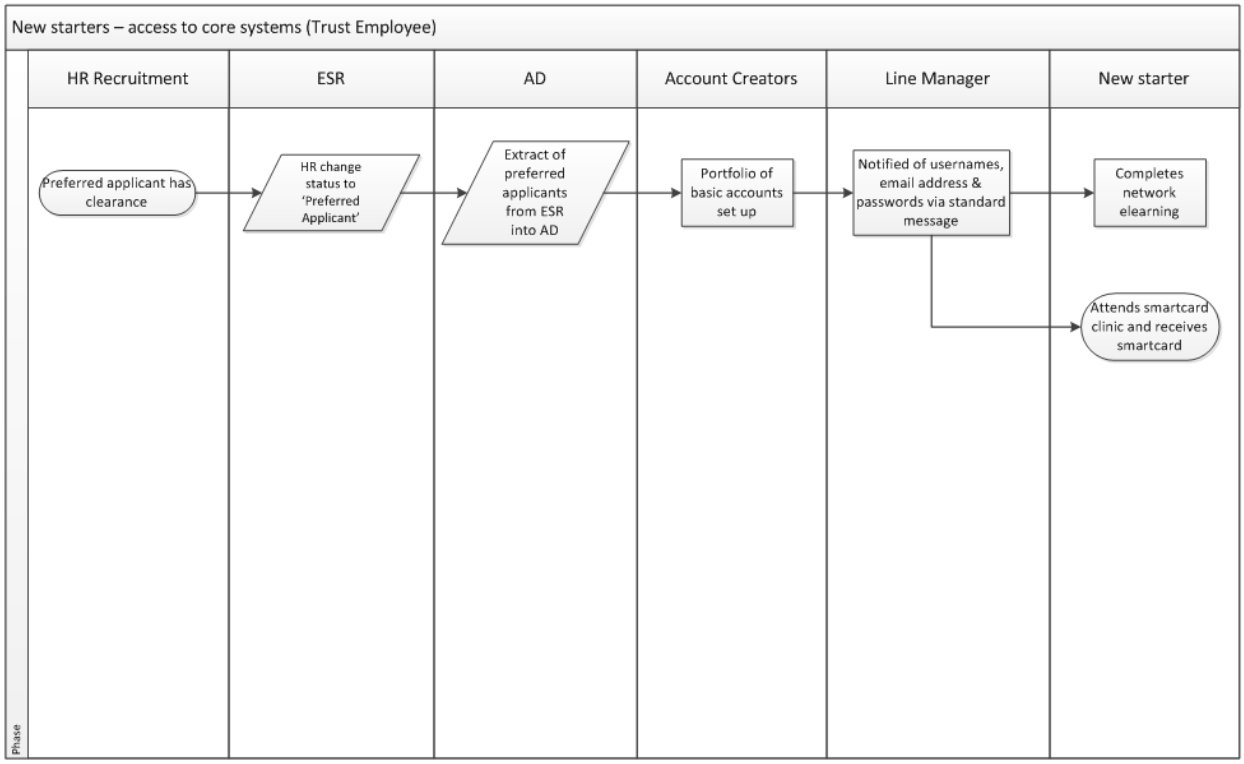
4 Related documents

- Data Protection Act 1988
- Freedom of Information Act 2000 Policy and Procedure
- Registration Authority Policy and Procedures
- Retention and Disposition of Records Procedure
- Network Access and User Operational Procedure
- Information Security Policy
- ESR System Specific Policy
- Email Policy and Procedure
- Confidentiality Code of Practice
- Information Governance Policy
- Data Protection Policy
- Record Management Lifecycle Policy
- Clear desk policy
- ESR document M-100 Trust site IT printer and network infrastructure readiness

5 Using the system

5.1 Access to ESR

The process for granting access to ESR is outlined in the diagram below:



5.1.1 Who can have access to the ESR System?

All Trust staff members can have access to employee self-service to view their own personnel record and e-learning to subscribe to required online training. Staff members with a legitimate need to view and/or record other staff information for their role will be given additional access once their line manager verifies this.

N.B any exceptions can only be approved by the Trust Caldicott guardian.

For ESR to be fully effective and accurate all staff and managers are to update ESR through Self Service in a timely manner

5.1.2 Obtaining access to the ESR system

For new members of staff, the individual's line manager arranges access to ESR as part of the local induction process. Access to ESR requires:

- Receipt of a valid SmartCard/Virtual Smartcard

In addition, access to core modules of ESR and manager self-service will require the completion of a OneForm, submitted via the Service Desk self-service portal.

5.1.3 Supervisor & Administrator Self Service

Access to Supervisor and Administrator self-service is only available once the OneForm is authorised by the line manager and submitted via the Service Desk. The Corporate Systems team will provide requested access once all pre-requisite tasks have taken place. Further guidance on Supervisor Self Service and Administrator Self Service can be found on the Intranet or provided by contacting the Digital & Data Service Desk.

5.1.4 Manager Self Service

Access to Manager self-service is only available when the following prerequisites have been met:

- An AS Number has been setup by Finance (An AS number request form can be found within the Finance pages on the Intranet)
- OneForm authorised by line manager is submitted to the Corporate Systems team via the self-service portal.

Further guidance on Supervisor Self Service and Administrator Self Service can be found on the Trust intranet or provided by contacting the Digital & Data Service Desk.

5.2 Removing access to ESR

For staff leaving the Trust, access to ESR is removed as part of the Leavers process. If urgent removal of access is required, for example, in instances of investigation or disciplinary, the manager must log a request with the Digital & Data service desk.

5.3 Passwords

Access to ESR is provided through using a SmartCard/ Virtual Smartcard.

Under no circumstances should you allow anyone else to access the system using your SmartCard and password. Disclosure of passwords to others could lead to disciplinary action

Trust staff can access ESR with username and password. They can gain this information in the ESR Hub and selecting forgotten username/password. An email address must have been added to ESR by Workforce Information prior to this.

6 Security

Line managers are responsible for ensuring that staff members have undertaken and passed relevant mandatory and statutory training and are aware of the organisations policies and procedures, especially related to information security. This will ensure they understand the Trust's data governance, legal and ethical requirements for protecting and accessing personal information. Trust terms and conditions of employment include adherence to Information Governance standards, information security requirements, code of confidentiality and common law of confidentiality.

ESR contains staff-identifiable information.

You are responsible for maintaining the confidentiality of information relating to staff. Please refer to the Trust's policy for Confidentiality and Sharing information.

7 Managing ESR

7.1 Planned downtime

Downtime will be planned well in advance and notice given to system users to make alternative arrangements as defined by service business continuity plans. The system will generally be available 24 hours per day from Trust-networked sites.

7.2 Emergency downtime

There will be occasions where the system is unavailable due to unplanned downtime. On these occasions, end users should inform the Service Desk and invoke Business Continuity Plans.

The logging of a call to the Service desk will usually identify ESR unavailability and escalation of issues to the system suppliers dedicated helpdesk portal. Incidents are classed as critical, high, moderate, or standard, depending on the severity of business impact.

If ESR is unavailable, end users should revert to their operational department business continuity policies. These may include, but not be limited to, the use of other Trust locations, use of reciprocal agreements with other Trusts or the use of manual paper systems in the interim period prior to fault resolution being achieved. All operational areas using ESR should hold signed, up to date business continuity plans.

8 ESR System Monitoring

The ESR system is fully auditable, and access is monitored.

Staff records are restricted to those who are defined as the individuals 'line manager'. In some instances, the manager may have delegated the updating of the ESR system to an appropriate administrator using administrator self-service.

Line managers can view their team/wards key performance indicators via the IIC. Any request for further reporting should be made via the Service Desk.

9 Audit

ESR will be subject to regular audit in the following areas:

- General systems control audit – URP (User Responsibility Profile) audit every six months. The last audit was completed October 2022. The next audit is scheduled for April 2023.
- The Digital & Data department is also required to access ESR for the purpose of support call resolution and information analysis.
- Any other audit to check the system is being used appropriately and securely.

10 Terms and definitions

Term	Definition
IBM	• The company responsible for the provision and operation of the ESR system
Smartcard/Virtual Smartcard	• An electronic device, the size of a credit card, that contains memory and an embedded integrated circuit or a virtual smartcard which is a form of physical smartcard which can be stored on a device, smartphone, or cloud. Smartcards are needed to use the ESR system and other services to ensure confidentiality and appropriate access levels are maintained
TPLY (Test Production Live Environment)	• Replicated ESR system used for testing
User Responsibility Profile (URP)	• URP's are specific forms/areas within ESR which allow users to access staff records and amend data as necessary.

11 How this procedure will be implemented

- This policy will be published to the Trust Intranet

11.1 Training needs analysis

Staff/Professional Group	Type of Training	Duration	Frequency of Training
Manager Self Service	Videos/user guides	As and when required	As and when required
Supervisor Self Service	Videos/user guides	As and when required	As and when required

12 How the implementation of this procedure will be monitored

Number	Auditable Standard/Key Performance Indicators	Frequency/Method/Person Responsible	Where results and any Associate Action Plan will be reported to, implemented and monitored; (this will usually be via the relevant Governance Group).
1	Monitoring of service requests	During BAU Requests. Corporate Systems Team.	
2	Regular HR, System and Payroll reporting	Monthly. Corporate Systems Team.	

13 References

ESR User Manual is available on the ESR dashboard Home - ESR Hub - NHS Electronic Staff Record

All user guides and related material can be found on the ESR Hub.

14 Document control (external)

To be recorded on the policy register by Policy Coordinator

Date of approval	25 April 2023
Next review date	25 April 2026
This document replaces	IT-0031-003-v2 ESR Procedure
This document was approved by	DPAG review meeting
This document was approved	25 April 2023
This document was ratified by	n/a
This document was ratified	n/a
An equality analysis was completed on this policy on	03/02/2023
Document type	Public
FOI Clause (Private documents only)	n/a

Change record

Version	Date	Amendment details	Status
v3	25 Apr 2023	Full review with changes throughout	Approved

Appendix 1 - Equality Analysis Screening Form

Please note: The Equality Analysis Policy and Equality Analysis Guidance can be found on the policy pages of the intranet

Section 1	Scope
Name of service area/directorate/department	Digital & Data
Title	Electronic Staff Record Procedure
Type	Procedure/guidance
Geographical area covered	Trust Wide
Aims and objectives	Provide information and appropriate use and access to ESR.
Start date of Equality Analysis Screening	03/02/2023
End date of Equality Analysis Screening	03/02/2023

Section 2	Impacts
Who does the Policy, Service, Function, Strategy, Code of practice, Guidance, Project or Business plan benefit?	All System Users, Digital & Data department
Will the Policy, Service, Function, Strategy, Code of practice, Guidance, Project or Business plan impact negatively on any of the protected characteristic groups?	• **Race** (including Gypsy and Traveller) **NO** • **Disability** (includes physical, learning, mental health, sensory and medical disabilities) **NO** • **Sex** (Men, women and gender neutral etc.) **NO** • **Gender reassignment** (Transgender and gender identity) **NO** • **Sexual Orientation** (Lesbian, Gay, Bisexual, Heterosexual, Pansexual and Asexual etc.) **NO** • **Age** (includes, young people, older people – people of all ages) **NO**

	• **Religion or Belief** (includes faith groups, atheism and philosophical beliefs) **NO** • **Pregnancy and Maternity** (includes pregnancy, women who are breastfeeding and women on maternity leave) **NO** • **Marriage and Civil Partnership** (includes opposite and same sex couples who are married or civil partners) **NO** • **Armed Forces** (includes serving armed forces personnel, reservists, veterans and their families) **NO**
Describe any negative impacts	N/A
Describe any positive impacts	N/A

Section 3	**Research and involvement**
What sources of information have you considered? (e.g. legislation, codes of practice, best practice, nice guidelines, CQC reports or feedback etc.)	N/A
Have you engaged or consulted with service users, carers, staff and other stakeholders including people from the protected groups?	No
If you answered Yes above, describe the engagement and involvement that has taken place	
If you answered No above, describe future plans that you may have to engage and involve people from different groups	N/A

Section 4	**Training needs**

As part of this equality analysis have any training needs/service needs been identified?	No
Describe any training needs for Trust staff	N/A
Describe any training needs for patients	N/A
Describe any training needs for contractors or other outside agencies	N/A

Check the information you have provided and ensure additional evidence can be provided if asked

Appendix 2 – Approval checklist

	Title of document being reviewed:	Yes / No / Not applicable	Comments
1.	**Title**		
	Is the title clear and unambiguous?	Yes	
	Is it clear whether the document is a guideline, policy, protocol or standard?	Yes	
2.	**Rationale**		
	Are reasons for development of the document stated?	Yes	
3.	**Development Process**		
	Are people involved in the development identified?	Yes	
	Has relevant expertise has been sought/used?	Yes	
	Is there evidence of consultation with stakeholders and users?	No	
	Have any related documents or documents that are impacted by this change been identified and updated?	Yes	
4.	**Content**		
	Is the objective of the document clear?	Yes	
	Is the target population clear and unambiguous?	Yes	
	Are the intended outcomes described?	Yes	
	Are the statements clear and unambiguous?	Yes	
5.	**Evidence Base**		
	Is the type of evidence to support the document identified explicitly?	Yes	
	Are key references cited?	Yes	
	Are supporting documents referenced?	Yes	
6.	**Training**		
	Have training needs been considered?	Not Applicable	
	Are training needs included in the document?	Not Applicable	
7.	**Implementation and monitoring**		

	Title of document being reviewed:	Yes / No / Not applicable	Comments
	Does the document identify how it will be implemented and monitored?	Yes	
8.	**Equality analysis**		
	Has an equality analysis been completed for the document?	Yes	
	Have Equality and Diversity reviewed and approved the equality analysis?	Yes	
9.	**Approval**		
	Does the document identify which committee/group will approve it?	Yes	
10.	**Publication**		
	Has the policy been reviewed for harm?	Yes	
	Does the document identify whether it is private or public?	Yes	public
	If private, does the document identify which clause of the Freedom of Information Act 2000 applies?	Yes	