NHS
St Helens and Knowsley Teaching Hospitals
NHS Trust

Electronic Staff Records Procedure Document

Document Summary
To provide regulations and guidance for access, security and use of the Electronic Staff Record (ESR) system.

DOCUMENT VERSION	V1
DOCUMENT AUTHOR	Joanne Powell Head of Service Delivery ESR & Workforce Systems
TARGET AUDENCE	Trust wide users of Electronic Staff Record (ESR) System
KEY WORDS	Electronic Staff Records, ESR, Access, Guidance, Security
DATE PUBLISHED	30th June 2021
DATE OF REVIEW	30th June 2023

Important Note:

The Intranet version of this document is the only version that is maintained.

Any printed copies should therefore be viewed as "uncontrolled" and, as such, may not necessarily contain the latest updates and amendments.

CONTENTS

1 PURPOSE

The purpose of this document is to provide regulations and guidance for the specific access, security and use of the Electronic Staff Record (ESR) system in use within St Helens and Knowsley Teaching Hospitals Trust (STHK).

Misuse of ESR can compromise the Trust's confidential information, staff information and otherwise adversely affect the Trust's interests and reputation.

There are several electronic systems that hold personnel data. This document only relates to the use of ESR.

2 WHO CAN HAVE ACCESS TO THE ESR SYSTEM

All Trust members can have access to employee self-service to view their own personnel record and subscribe to any 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.

For ESR to be fully effective records must be updated in a timely manner.

3 OBTAINING ACCESS TO ESR

EMPLOYEE SELF SERVICE

For new member of staff to access Employee Self Service an email is to be sent to the ESR.Helpdesk@sthk.nhs.uk inbox. This must contain the employees full name, date of birth, and first 4 digits of their national insurance number. This is to ensure that the correct user account details are given.

CORE FUNCTIONS

Staff who requires access to core functionality in ESR will only be granted once the following pre-requisites have been met:

- Receipt of a valid active Smartcard
- Successful completion of an ESR06 User Access Form
- Successful completion of an ESR Confidentiality Declaration Form (Core Users)

Further guidance on core functions can be obtained from the Electronic Staff records Access Control Procedure document or by contacting the ESR & Workforce Systems team.

MANAGER SELF SERVICE

Staff who requires access to Manager Self Service will only be granted once the following pre requisites have been met:

- Receipt of a valid active Smartcard
- Successful completion of an ESR06 User Access Form
- Successful completion of an ESR Confidentiality Declaration Form (Core Users)

Further guidance on core functions can be obtained from the Electronic Staff records Access Control Procedure document or by contacting the ESR & Workforce Systems team.

Training is available upon request by contacting the ESR & Workforce Systems team. A suite of guidance documents are also available on the ESR & Workforce Systems intranet pages.

A link to the guidance can be obtained in the link below:

Manager Self Service Guidance

SUPERVISOR & ADMINISTRATOR SELF SERVICE

Staff who require access to Supervisor or Administrator Self Service will only be granted once the following pre requisites have been met:

- Receipt of a valid active Smartcard
- Successful completion of an ESR06 User Access Form
- Successful completion of an ESR Confidentiality Declaration Form (Core Users)

Further guidance on core functions can be obtained from the Electronic Staff records Access Control Procedure document or by contacting the ESR & Workforce Systems team.

Training is available upon request by contacting the ESR & Workforce Systems team. A suite of guidance documents are also available on the ESR & Workforce Systems intranet pages.

A link to the guidance can be obtained in the link below:

Supervisor & Administrator Self Service Guidance

4 REMOVING ACCESS TO ESR

For staff leaving the Trust, access to ESR is removed as part of the organisations termination process. If urgent removal of access is required , for example in instances of investigation or disciplinary, the manager must request this with the ESR & Workforce Systems team.

5 PASSWORDS

Access to ESR for core users is via a Smartcard, which is accessed via a passcode. Access to Employee Self Service with no core functionality is via username and password.

Under no circumstances must the user allow anyone else to access the system using their Smartcard, or username and password. It is the responsibility of the user to ensure that their details are kept confidential. Disclosure and inappropriate use of Smartcards could result in disciplinary action.

6 SECURITY

Line managers are responsible for ensuring staff has undertaken the relevant statutory and mandatory training and are aware of the organisations policies and procedures, especially relating 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 confidentiality.

ESR contains staff identifiable information and therefore users are responsible for maintaining the confidentiality of information relating to staff. Please refer to the Trusts Confidentiality Code of Conduct policy.

Confidentiality Code of Conduct Policy

7 MANAGING ESR

PLANNED DOWNTIME

There are clear service standards to monitor planned downtime of the ESR system to enable maintenance and updates. In the main this will be planned well in advance and notice given to system users. A notification via the Trust's IT Notification system will be issued to notify of any downtime to enable staff to make alternative arrangements The system will generally be available 24 hours per day.

8 EMERGENCY DOWNTIME

There will be occasions where the system is unavailable and prior notice has not been given. On these occasions you should inform the ESR & Workforce Systems team and invoke your Business Continuity Plan.

The logging of an issue with the ESR & Workforce Systems team will usually identify ESR unavailability and escalation of issues via the system supplier's helpdesk portal. Faults are classed as critical, high, moderate or standard depending on the severity of business impact. The system supplier will respond to the helpdesk calls logged within the agreed timescales. The ESR & Workforce Systems team will notify of the outcomes and timescales via the IT Helpdesk and an IT Notification announcement will be issued to all users.

If ESR is unavailable and no functionality can be accessed all users should revert to their operational departmental business continuity plan. These may include but not limited to the use of manual paper systems in the interim period prior to fault resolution being achieved. All operational areas using ESR should hold up to date business continuity plans.

9 ESR SYSTEM MONITORING

The ESR system is fully auditable and access is monitored.

Staff records are restricted to those who have been defined as a 'Line Manager'. In some instances managers 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 IPR system. Several appropriate business intelligence reports are available within ESR for managers to run. Any further requests for reporting should be made via the ESR & Workforce Systems team.

10 AUDIT

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

- General systems control audit – security, access, and passwords, system administration controls
- The ESR & Workforce Systems team is also required to access ESR to review usage of the system for the purpose of support call resolution and information analysis.
- Any other audit to check the system is being used appropriately and securely.

11 RELATED DOCUMENTS

- Equality & Human Rights Policy
- Confidentiality Code of Conduct Policy
- Corporate Records Management Policy
- Information Governance Policy
- Disciplinary Policy
- Records Management Code of Practice for Health & Social Care