The Shrewsbury and Telford Hospital NHS Trust

Maintaining Personal Files and Electronic Staff Records

Policy W27

Additionally refer to	Verification of Professional Registrations Recruitment and Selection Policy Disclosure & Barring (DBS) Service Disciplinary Policy Equality, Diversity & Inclusion Policy Access to Records and Individual Rights to Personal Data

Version:	V4
V1 issued	April 2007
V3 approved by	JNCC
V4 date approved	February 2023
V4 Ratified by:	Director of People & OD
V4 Date ratified:	February 2023
Document Lead	People Governance & Projects Manager
Lead Director	Director of People & OD
Date issued:	February 2023
Review date:	February 2026
Target audience:	All Staff

Version Control Sheet

Document Lead/Contact:	People Governance & Projects Manager sath.hradvice@nhs.net
Document ID	W27
Version	4
Status	Final
Date Equality Impact Assessment completed	January 2023
Issue Date	February 2023
Review Date	February 2026
Distribution	Please refer to the intranet version for the latest version of this policy. **Any printed copies may not necessarily be the most up to date**
Key Words	Maintain, Personal, Records, ESR, Information, Employee, Staff, Files
Dissemination	Staff Briefing, placed on internet and or intranet; email to managers resources list.

Version history

Version	Date	Author	Status	Comment
V1	April 2007	HRIS Manager	FINAL	Approved by JNCC
V1	May 2007	HRIS Manager	FINAL	Approved by Board
V2	2013	Jenny Deakin	FINAL	Amendments to sections: 1, 3, 4.3, 4.4, 5.1, 5.2, 6.1, 6.2, 7.2, 8.1, 9.1, 9.2, 9.3, and Appendix A
V3	Nov 2022	People Governance & Projects Manager	Draft	Reviewed over past 12 months, input from various parts of People & OD team and IG team.. Data Protection Act updated to GDPR.
V4	Dec 2022	People Governance & Projects Manager	Draft	Minor amendments following WPPG.
V4	Feb 2023	People Governance & Projects Manager	FINAL	Approved at JNCC.

Contents

1 Policy on a Page

- The purpose of this policy is to provide a standard for the way the Trust maintains personal files.
- This Policy applies to all staff employed by the Trust. Arrangements for Medical and Dental staff will be coordinated by the Medical People Services Team. The policy does not apply to external contractors or agency staff.
- The General Data Protection Regulation (GDPR), together with a new Data Protection Act 2018, will replace all pre-existing provisions under the Data Protection Act 1998.
- The Trust acts as a Data Controller and must adhere to GDPR and the Data Protection Act 2018. This will impact on how employers process, manage and store personal data.
- Managers are responsible for ensuring that personal files are kept up to date and information contained is relevant.
- Employees are responsible for informing their manager in writing of any changes in personal details.
- It is the responsibility of the line manager to ensure that all manual and electronic employment records are kept safe and secure, with access by staff that have designated authority.

2 Scope

2.1 This Policy applies to all staff employed by the Trust. Arrangements for Medical and Dental staff will be coordinated by the Medical People Services Team. It does not apply to external contractors or agency staff.

2.2 In implementing this policy, managers must ensure that all staff are treated fairly and within the provisions and spirit of the Trust's Equality, Diversity and Inclusion Policy.

3 Definitions

3.1 General Data Protection Regulations (GDPR)

GDPR brings about a number of changes which will impact on how employers process, manage and store personal data. The GDPR, together with a new Data Protection Act 2018, will replace all pre-existing provisions under the Data Protection Act 1998.

3.2 Personal Data

Personal data means data which relates to a member of staff who can be identified from the data and other information that is held by the Trust about them. The GDPR defines personal data as:

- Relating to a living human being who can be directly or indirectly identified.
- Identifiers include ID numbers, location data, physical, psychological, genetic, mental factors, this may include (but is not limited to):
    - Name
    - Date of Birth
    - Postcode
    - Address
    - National Insurance Number
    - Photographs, digital images etc.
    - NHS Number
    - Hospital Number
    - Date of Death
    - Passport Number
    - Online Identifiers and location data (such as MAC, IP addresses and mobile device ID's

Definition of Special Categories data

Categories of information are classified as special categories of personal data and require additional safeguards '*formerly sensitive data'* when sharing or disclosing this information in line with guidance and legislation. This includes (but is not limited to):

- Concerning health, sex life or sexual orientation.
- Racial or ethnic origins.
- Trade union membership.
- Political opinions.
- Religious or philosophical beliefs.
- Genetic / Biometric data.

3.3 Data Controller

A living human or legal person, public authority, agency or other body who determines the purposes and means of processing data. The Trust is the Data Controller and must adhere to GDPR.

3.4 Data Subject

A human being who can be identified directly or indirectly, in particular by reference to an identifier (such as name, identification number, location number or some other factor).

3.5 The Electronic Staff Record (ESR)

The ESR programme is a Department of Health (England) system, providing an integrated HR and Payroll system used across the whole of the NHS in England and Wales.

The 'ESR workforce records' functionality encompasses the three major areas of workforce management – new joiners, variations and leavers. The information held includes employee demographic and personal details (e.g. name, address, emergency contacts, equal opportunities data, competencies, work experience, employment history, memberships and qualifications) and assignment information (e.g. grade, post, contracted hours, place of work, annual leave, benefits, absence, salary).

3.6 CRS Smartcard

NHS Care Records Service (CRS) Smartcards controls access to ESR. Smartcards are similar to a chip and PIN credit or debit card but are more secure as they do not use a magnetic strip and have an alphanumeric Passcode rather than a PIN. A Smartcard is printed with the user's name, photograph and unique identifier number.

3.7 Retention

Retention is the period of time a document should be kept or "retained" both electronically and in paper format (see section 9).

3.8 Disposal

Documents which have reached the end of their administrative life should be destroyed in as secure a manner as required by the Records Management Code of Practice for Health and Social Care 2016.

4 Responsibilities

4.1 Chief Executive and Directors

The Chief Executive and the Executive Board have an overall responsibility to oversee this Policy and to ensure its correct application.

4.2 Data Protection Officer

The Trusts Data Protection Officer will monitor internal compliance with the Data Protection Act and GDPR. They will provide advice on the Data Protection Law, Data Protection Impact Assessments (DPIAs) and act as a contact point for data subjects and the supervisory authority.

4.3 People & OD Directorate

The Director of People & OD has overall responsibility for this policy.
The People Advisory Team will have a responsibility to provide advice in relation to the application of this policy and relevant employment law and best practice.

4.4 Managers

All managers are responsible for ensuring that:

- They comply with the requirements of this Policy and where this policy interacts with other related policies of the Trust.
- Personal files for the employees who they directly manage are kept up to date and information contained is relevant and in line with Appendix A.
- Staff have access to their personal files on request as per the Access to Records and Individual Rights to Personal Data Policy .
- The security of the personal file for all employees they manage is maintained.
- The relevant ESR form is completed and forwarded to sath.esr@nhs.net following changes of contractual and personal details.
- The personal file is forwarded to the relevant manager where a member of staff transfers internally within the Trust.

- They will not divulge any personal information about an individual to anyone in the Trust or external source other than for the purposes of references, management of an individual or with the individual's consent.

4.5 Staff

Employees are responsible for informing the Trust of any changes in personal details relevant to their employment, for example:

- *Change of address or telephone number
- *Change in the name/address of emergency contact details
- *Change in bank details
- Achievement of any professional qualifications (certificates should be stored on the personal file).
- Professional Registration details
- Change in name (requires manager approval and appropriate evidence of change seen by the manager and stored in the personal file or on ESR)
- Change in residency status (requires manager approval and appropriate evidence of change seen by the manager and stored in the personal file or on ESR)

These may be updated by notifying the line manager in writing, or those marked with a * can be updated by the employee themselves using ESR Employee Self Service.

5 Legislation

5.1 GDPR

The GDPR significantly updates the provisions outlined in the EU's pre-existing data protection directive, which forms basis of the Data Protection Act 1998. It is intended to strengthen and unify data protection for all individuals within the EU.

In addition to EU- based organisations, these requirements will also apply to any company in any country that has responsibility for processing the personal data of EU citizens, including where this relates to the delivery of goods, services or profiling.

5.2 GDPR Principles.

The controller shall be responsible for, and be able to demonstrate compliance with the following principles regarding to personal data:

- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- Accurate and, where necessary, kept up to date. Inaccurate data must be erased or rectified without delay.
- Kept in a form permitting, identification of data subjects for no longer than necessary for the purposes for which the personal data are processed.
- Processed in a manner that ensures appropriate security of the personal data, including protection against accidental loss, destruction or damage using appropriate technical or organisational measures.

5.3 Lawful processing of Personal Data

Data can be processed under following legitimate reasons:

- Consent given by data subject

- Performance of a contract where the Data Subject is party to the contract or in order to take steps at the request of the data subject prior to entering into a contract.
- Compliance with a legal obligation to which the controller is subject.
- Protect vital interests of the data subject or other natural person.
- Performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- Purposes of legitimate interests pursued by the controller or third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject.

Further information relating to the processing of personal data can be found within the employee privacy notice on the intranet.

5.4 Lawful processing of Special Category Data

Processing of special category data is prohibited unless one of the following conditions apply:

- Data subject has given consent
- Necessary for carrying out obligations of the controller or data subject in relation to employment, social security and social protection law.
- Protect vital interests of data subject.
- Legitimate activities of not-for-profit body with political, philosophical, religious of trade union aim and relates to processing of members/former members
- Personal data made public by the data subject
- Defence of legal claims
- Necessary for substantial public interest.
- Necessary for the purposes of preventative or occupational medicine, for assessment of working capacity of employee, medical diagnosis, provision of health or social care system services.
- Public interest in public health
- Archiving purposes in public interest, scientific or historical research purposes.

Further information relating to the processing of special category data can be found within the employee privacy notice on the intranet.

5.5 Individual Rights

Data subjects must be informed about what data is collated, for what purpose and who this may be shared with. For details please refer to the Employee Privacy Notice that can be found on the Workforce Home page on the Trust Intranet.

Data subjects have the following rights under GDPR:

- Right to access
- Request rectification of data that is inaccurate or incomplete.
- Request erasure, specific reasons must apply.
- Restrict processing of personal data.
- Right to data portability
- Object to processing if it is not based on public interest or legitimate interest.

Further information relating to your rights, can be found with the Data Protection, GDPR and Confidentiality Policy.

5.6 Access to Personal Files (Subject Access Requests)

Staff have the right to obtain the following:

- confirmation that the Trust are processing their personal data;
- a copy of their personal data; and
- other supplementary information

Copies of files will be provided within 1 month of receiving the request, but this is extendable to two months for complex requests. All subject access requests should follow the guidance within the Access to Records and Individual Rights to Personal Data Policy.

5.7 Personal Data Breach Notification

When a personal data breach has occurred, the likelihood and severity of the resulting risks to people's rights and freedoms will need to be assessed. If there is likely to be a risk then the Trust shall notify the Information Commissioning Office within 72 hours after becoming aware of the personal data breach. If it is unlikely that there is a risk then you do not have to report it but you will need to justify your decision so you should document it. The Data Protection Officer will be able to provide advice should breaches occur.

The breach will then be reported to the data subject:

- without undue delay
- when personal data breach is likely to result in a high risk to the rights and freedoms of the data subject
- Not necessary if measures are taken to ensure the high risk is no longer likely to materialise.

6 Computerised Files (including ESR and other Local Databases)

6.1 ESR and other local databases, records staff details relating to:

- Recruitment and Selection
- Job details and pay
- Employment (including promotion, transfers, disciplinary procedures, termination and redundancy)
- Training and Development.
- Personal details (see para 4.4)
- Career progression.

6.2 ESR records are held nationally and can be transferred via an Inter Authority Transfer when an employee leaves the Trust to take up employment within another NHS organisation.

7 Security of Files

7.1 It is the responsibility of the line manager to ensure that all manual and electronic employment records are kept safe and secure, with access only by staff that have designated authority.

7.2 Computerised records MUST be protected by a system of passwords or accessed via a CRS smartcard and only authorised staff should have access to these records. When leaving the workstation staff must log off or lock their workstation, in order to ensure security of data.

7.3 Following a full and proper investigation, any breaches of security or confidentiality identified will be treated as a disciplinary issue in line with the Trust's Disciplinary Policy.

8 Confidentiality

8.1 All the information contained within the employee's personal file whether it is manual or computerised is treated as confidential. However, the Trust has a statutory duty to supply legally required information to certain government agencies or departments such as the Inland Revenue or the DWP or for information required in a disciplinary investigation.

8.2 If an outside agency e.g., Bank or Building Societies contact the Trust for information, the employees' written consent must be obtained before the information is supplied.

8.3 Following a full and proper investigation, any breaches of confidentiality identified will be treated as a disciplinary issue.

9 Retention and Disposal

9.1 Personal records are classed as major records, including records such as, letters of appointment, contracts, references and related correspondence, registration authority forms, training records and equal opportunity monitoring records (if retained) (including those for locum doctors). The minimum retention period for these records is 6 years after the individual leaves service, at which time a summary (see 9.2) of the file must be kept until the individual's 70th birthday, or until 6 years after end of employment if aged over 70 years at the time.

9.2 The summary should contain everything except attendance books, annual leave records, duty rosters, clock cards, timesheets, study leave applications, training plans. These are considered minor records and can be removed 2 years after the year to which they relate.

Executive and Non-Executive Directors' personal files must be retained permanently.

9.3 Where records exceed their retention period they should be destroyed as soon as possible using confidential data shred bins which are then destroyed in a secure manner.

A record of the destruction of records, showing their reference, description and date of destruction should be maintained and preserved by the relevant manager, so that the Trust is aware of those records that have been destroyed and are therefore no longer available.

9.4 If an employee submits evidence as part of a HR process (e.g. grievance, disciplinary) this may be retained within their personal file and/or stored securely (electronically or hard copy) by the People Directorate. If the evidence contains personal data, employees can request that this is deleted or returned to them at the end of the process. The People Directorate will confirm in writing when this has been completed.

10 Training Needs

There is no mandatory training associated with this policy. However, the Trust does hold mandatory Data Security Awareness training. If staff have any queries this policy, they should contact their line manager in the first instance. Advice may also be sought from the People Advisory Team.

11 Review process

The Trust will review this policy every 3 years, unless there are significant changes at either a national policy level, or locally. In order that this document remains current, any of the appendices to the policy can be amended and approved during the lifetime of the document without the document strategy having to return to the ratifying committee.

12 Equality Impact Assessment (EQIA)

An Equality Impact Assessment has been carried out on this policy which has been found not to discriminate against any groups of staff or potential members of staff.

13 Process for monitoring compliance

Aspect of compliance or effectiveness being monitored	Monitoring method	Responsibility for monitoring (job title)	Frequency of monitoring	Group or Committee that will review the findings and monitor completion of any resulting action plan
Types of check required	Capture and analysis of personal files for all staff including fixed term /temporary staff Minimum of 2 files per specialty /department per Centre	HR link for each Centre/Department	Annual	Operational People Group
Checking procedures		HR link for each Centre/Department	Annual	Operational People Group
Process for following up those who fail to satisfy the checking arrangements		HR link for each Centre/Department	Annual	Operational People Group

14 References

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/
The principles of the Data Protection Act in detail

http://intranet/information_governance/ig_policies.asp
Records Management – NHS Code of Practice

http://www.connectingforhealth.nhs.uk/systemsandservices/rasmartcards
Registration Authority and Smartcards

https://my.esr.nhs.uk/dashboard/web/esrweb
Electronic Staff Record

http://www.nhsemployers.org/RecruitmentAndRetention/Employment-checks/Employment-Check-Standards/Pages/Employment-Check-Standards.aspx
NHS Employment Check Standards

https://www.gov.uk/government/organisations/disclosure-and-barring-service/about
Disclosure and Barring Service

Appendix A Contents of an Employment Personal File

Personal files help to ensure staff receive their correct pay, holiday, pension and other entitlements and benefits. They can be used to monitor fair and consistent treatment for staff. Below is checklist for the Data to be held on Personal files (this list is not exhaustive):

1) **Advertisement** - for the post that individual was recruited.
2) **Person Specifications** - for all posts an employee has held
3) **Job Descriptions** - for all posts an employee l has held
4) **Application Form** – a record that an employee l has confirmed that information given is correct and accurate at the time
5) **References** – under the GDPR copies of original references, obtained for vetting purposes as part of the recruitment process should only be held for up to 6 months. They should then be securely destroyed. A record may be kept of the date references were requested/received; from whom, and the recruitment decision made.
6) **Medical Clearance** - declaration from Occupational Health
7) **Recruitment Checklist** – tracking the progress of the recruitment process
8) **Correspondence** – invite to interview letter; offer of appointment letter; acceptance letter; and DBS Memo.
9) **Induction programme** – this should include details of attendance at the Trust Induction Programme and any specific training programmes attended . It will also include any individual/local induction checklists, a record/confirmation that the employee received copies of relevant work documentation.
10) **A copy of the ESR New Starter Form**
11) **Terms and Conditions of Employment (the employment 'contract')** – two copies should be issued– one for retention by the individual, the other should be retained on the personal file.
12) **Professional Registration Details** – a copy of the online check and any updates should be held on the file.
13) **Copy of Driving Licence and relevant car insurance details** (if appropriate to job role)
14) **Proof of Identity** – see the NHS Employment Check Standards
15) **Change Forms** – these should be followed up by a variation to contract letter if appropriate and a copy retained on file.
16) **Medical Certificates** – self certificates and those issued by GPs, Hospitals.
17) **A copy of an online right to work check and passport** – documentations confirming eligibility to work in the UK (where necessary).
18) **Documentation appertaining to authority to reside in the UK** (where applicable).
19) **Copies of Qualifications –** those relevant to the post including all those specified as being required in the person specification.
20) **Correspondence** – relating to the employee's employment
21) **Disciplinary Record Documentation** – relating to disciplinary action taken against the member of staff, in accordance with the Trust's Disciplinary Policy Disciplinary and other investigation files will be retained within the People Advisory Team.
22) **Individual Performance Reviews/Appraisals/Personal Development Plans.**
23) **Study Leave Forms** or details of any training/development undertaken.
24) **Sickness Absence** – for the current year these may be held centrally but at the end of each year this should be transferred to the employee's personal file. Documentation should include Return to Work Interviews. It should also include any information/correspondence received/obtained in connection with the employee's health and/or sickness absence.
25) **Annual Leave** – for the current year these may be held electronically via the Health Roster System.
26) **Other Leave** – Records of other leave, including special leave and/or maternity leave taken, including the relevant application forms and approval notification. These may be stored on the personal file or on the Health Roster system. .
27) **Accident/Adverse Event Reports –** copies of any accidents or adverse events in which the employee has been involved during their employment.

28) **Grievance -** correspondence relating to grievances raised. Investigation files will be retained within the People Advisory Team.
29) **Employment Termination Records** – Employee resignation letter and copy of their ESR termination form.