Maintaining Personal Files and Electronic Staff Records

Human Resources Policy No. HR46

Additionally refer to
HR04 Verification of Professional Registrations
HR33 Recruitment and Selection
HR34 CRB Checks
HR36 Disciplinary Procedure
IG07 Subject Access Requests

<table>
<thead>
<tr>
<th>Version:</th>
<th>V2</th>
</tr>
</thead>
<tbody>
<tr>
<td>V1 issued</td>
<td>April 2007</td>
</tr>
<tr>
<td>V2 approved by</td>
<td>TNCC, PAG, HEC</td>
</tr>
<tr>
<td>V2 date approved</td>
<td>December 2013</td>
</tr>
<tr>
<td>V2 Ratified by:</td>
<td>Trust Board</td>
</tr>
<tr>
<td>V2 Date ratified:</td>
<td>30th January 2014</td>
</tr>
<tr>
<td>Document Lead</td>
<td>HR Information Systems Manager</td>
</tr>
<tr>
<td>Lead Director</td>
<td>Workforce Director</td>
</tr>
<tr>
<td>Date issued:</td>
<td>December 2013</td>
</tr>
<tr>
<td>Review date:</td>
<td>November 2015</td>
</tr>
<tr>
<td>Target audience:</td>
<td>All Staff</td>
</tr>
</tbody>
</table>

The original expiry date of this policy has been extended in agreement with staff side as we transition into a new policy consultation process.
Version Control Sheet

| Document Lead/Contact: | Jenny Deakin  
HR Information Systems Manager  
Jenny.Deakin@sath.nhs.uk |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Document ID</td>
<td>HR46</td>
</tr>
<tr>
<td>Version</td>
<td>2</td>
</tr>
<tr>
<td>Status</td>
<td>Final</td>
</tr>
<tr>
<td>Date Equality Impact Assessment completed</td>
<td>December 2013</td>
</tr>
<tr>
<td>Issue Date</td>
<td>December 2013</td>
</tr>
<tr>
<td>Review Date</td>
<td>December 2016</td>
</tr>
</tbody>
</table>
| 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 |
| Dissemination | Staff Briefing, placed on internet and or intranet; placed on notice board. |

Version history

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Author</th>
<th>Status</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>V1</td>
<td>April 2007</td>
<td>HRIS Manager</td>
<td>FINAL</td>
<td>Approved by TNCC</td>
</tr>
<tr>
<td>V1</td>
<td>May 2007</td>
<td>HRIS Manager</td>
<td>FINAL</td>
<td>Approved by Board</td>
</tr>
<tr>
<td>V2</td>
<td>2013</td>
<td>Jenny Deakin</td>
<td>FINAL</td>
<td>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</td>
</tr>
</tbody>
</table>
## Contents

<table>
<thead>
<tr>
<th>Paragraph</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Policy Statement</td>
</tr>
<tr>
<td>2</td>
<td>Scope</td>
</tr>
<tr>
<td>3</td>
<td>Definitions</td>
</tr>
<tr>
<td>4</td>
<td>Responsibilities</td>
</tr>
<tr>
<td>5</td>
<td>Legislation</td>
</tr>
<tr>
<td>6</td>
<td>Computerised Files (including ESR and other Local Databases)</td>
</tr>
<tr>
<td>7</td>
<td>Security of Files</td>
</tr>
<tr>
<td>8</td>
<td>Confidentiality</td>
</tr>
<tr>
<td>9</td>
<td>Retention and Disposal</td>
</tr>
<tr>
<td>10</td>
<td>Training Needs</td>
</tr>
<tr>
<td>11</td>
<td>Review process</td>
</tr>
<tr>
<td>12</td>
<td>Equality Impact Assessment</td>
</tr>
<tr>
<td>13</td>
<td>Process for monitoring compliance</td>
</tr>
<tr>
<td>14</td>
<td>References</td>
</tr>
</tbody>
</table>

**Appendices**

| Appendix A | Contents of an employment personal file | 9 |
1 Policy Statement
The purpose of this policy is to provide a standard for the way the Trust maintains personal files. The policy aims to ensure there is a consistent high standard, complying with all employment legislation. The policy details the entitlement of staff in relation to their personal files.

The policy seeks to promote good practice in the creation, maintenance and disposal of personal records. The policy aims to help the records manager understand the role that records play in the organisation, good personal records are necessary to allow the best use of available staff and promote efficiency in the organisation.

2 Scope
2.1 This Policy applies to all staff employed by the Trust. 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 Equal Opportunities Policy. Special attention should be paid to ensuring the policy is understood when using it for staff new to the NHS or Trust; by staff whose literacy or use of English is weak or for persons with little experience of working life.

3 Definitions
3.1 The Data Protection Act
The Data Protection Act 1998 is a UK Act of Parliament which defines UK law on the processing of data on identifiable living people.

The Act provides a broad framework of general standards that have to be met and considered in conjunction with other legal obligations. The Act regulates the processing of personal data, held both manually and on computer and incorporates eight data protection act principles.

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.

3.3 Data Controller
The Trust is the Data Controller. The Trust must adhere to the eight Data Protection Act principles for all personal data.

3.4 Data Subject
The Data Subject is the individual who is the subject of personal data.

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, changes and leavers. The information held includes employee demographic and personal details (e.g. name, address, emergency contacts, equal opportunities data, competencies, memberships and qualifications) and assignment information (e.g. grade, post, contracted hours, place of work, 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.

3.8 Disposal
Documents which have reached the end of their administrative life should be destroyed in as secure a manner as is appropriate to the level of confidentiality or protective markings they bear. This can be undertaken on site or via an approved contractor.

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 Human Resources
The Human Resources Department will have a responsibility to provide advice in relation to the application of this policy and relevant employment law and best practice.

4.3 Managers
All managers are responsible for ensuring that:
- They comply with the requirements of this Policy and related policies.
- Personal files are kept up to date and information contained is relevant.
- Any disciplinary letters with time limits are removed after the specified time.
- Staff have access to their personal files on request as per policy IG07.
- The security of the personal file is maintained.
- The relevant ESR form is completed (copy kept on file) and forwarded to the HRIS Team following confirmation of change 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 an employment reference, management of an individual or the individual has consented to the disclosure of their information to the person making the request.

4.4 Staff
Employees are responsible for informing their manager in writing (attaching documentary evidence where necessary) of any changes in personal details relevant to the Trust, for example:
- Change of address or telephone number
- Change in the name/address of emergency contact details
- Change in name
- Change in bank details
- Achievement of any professional qualifications
- Professional Registration details
- Change in residency status
5 Legislation

5.1 The Data Protection Act
The Data Protection Act sets a clear routine for processing personal information, applying to paper records and computerised records. The Act determines how personal information or data should be kept or treated and gives individuals (the “Data Subject”) greater control over how their personal information is gathered, used, housed and shared, while requiring those who record and use personal information (the “Data Controller”) to be open about how they use the information and to adhere to the Data Protection Act principles. The Act is based on eight principles as follows:

- Personal data shall be processed fairly and lawfully.
- Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose(s).
- Personal data shall be adequate, relevant and not excessive in relation to the purpose(s) for which they are processed.
- Personal data shall be accurate and, where necessary kept up to date.
- Personal data shall not be kept for longer than is necessary for the purpose for which it is collected.
- Personal data shall be processed in accordance with the rights of the data subjects under this Act.
- Appropriate technical and organisational measures should be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- Personal data shall not be transferred to countries outside the European Economic Area unless the country ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

5.2 Access to Personal Files (Subject Access Requests)
- The Data Protection Act allows members of staff to find out what information is held about them by the Trust. Staff are entitled to be given copies of all personal data held, if such a request is made please refer to IG07 policy.

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 employment records are kept in locked storage, with access by staff that have designated authority.
7.2 Computerised records e.g. ESR 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 identified will be treated as a disciplinary issue.

8 Confidentiality

8.1 All the information contained within the 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.

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 of the file must be kept until the individual’s 70th birthday, or until 6 years after cessation 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.

Minor Human Resources records, which include records such as attendance books, annual leave records, individual duty rosters, clock cards and timesheets must be retained (including those for locum doctors) for 2 years after the year to which they relate.

Executive and Non Executive Directors’ personal files must be retained permanently.

9.3 Personal records (including copies) not selected for archival preservation and which have reached the end of their administrative life should be destroyed in as secure a manner as is appropriate to the level of confidentiality or protective markings they bear. This can be undertaken on site or via an approved contractor.

A record of the destruction of records, showing their reference, description and date of destruction should be maintained and preserved by the Records Manager, so that the Trust is aware of those records that have been destroyed and are therefore no longer available. Disposal schedules would constitute the basis of such a record.
10 **Training Needs**
There is no mandatory training associated with this policy. If staff have queries about its operation, they should contact their line manager in the first instance.

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**

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

14 **References**

The principles of the Data Protection Act in detail

- [http://intranet/information_governance/ig_policies.asp](http://intranet/information_governance/ig_policies.asp)
Records Management – NHS Code of Practice

- [http://www.connectingforhealth.nhs.uk/systemsandservices/rasmartcards](http://www.connectingforhealth.nhs.uk/systemsandservices/rasmartcards)
Registration Authority and Smartcards

- [http://www.electronicstaffrecord.nhs.uk/home/](http://www.electronicstaffrecord.nhs.uk/home/)
Electronic Staff Record

- [http://www.nhsemployers.org/RecruitmentAndRetention/Employment-checks/Employment-Check-Standards/Pages/Employment-Check-Standards.aspx](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](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, holidays, 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 from
2) Person Specifications - for all posts individual has held
3) Job Descriptions - for all posts individual has held
4) Application Form – a record that the individual has confirmed that information given is correct and accurate at the time of giving
5) References – under the Data Protection Act 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 confidentially destroyed. A record may be kept of, a) the date references were requested/received; from whom, the result (but not the content) and the recruitment decision made.
6) Medical Clearance - declaration from Occupational Health
7) Recruitment Checklist – tracking the progress of the recruitment process
8) Disclosure and Barring Service (DBS) – The only information that can be kept on the personal record is:
   a) the level of check requested, including any checks against one or both of the barred lists
   b) the position for which the certificate was requested
   c) Date check for outcome was made on the electronic version of the database (available during 2013 – date to be specified)
9) Correspondence – invite to interview letter; offer of appointment letter; acceptance letter; and DBS Memo.
10) Induction programme – this should include details of attendance at the Trust Induction Programme and any specific programmes for that individual. It will also include any individual/local induction checklists including a record/confirmation that the individual has received copies of relevant work documentation.
11) A copy of the ESR New Starter Form
12) Terms and Conditions of Employment (the employment ‘contract’) – two copies should be issued within 8 weeks of commencement – one for retention by the individual, the other should be returned signed for retention on the personal file. A copy should also be held on the personal file pending receipt of the post holder’s signed copy.
13) Professional Registration Details – a copy of the registration card and any updates should be held on the file.
14) Copy of Driving Licence and relevant car insurance details (if appropriate)
15) Proof of Identity – see the NHS Employment Check Standards
16) Change Forms – these should be followed up by a variation to contract letter if appropriate and a copy retained on file.
17) Medical Certificates – self certificates and those issued by GPs, Hospitals.
18) A copy of a Visa and passport – documentations confirming eligibility to work in the UK (where necessary).
19) Documentation appertaining to authority to reside in the UK (where applicable).
20) Copies of Qualifications – those relevant to the post including all those specified as being required in the person specification.
21) Correspondence – relating to the individual’s employment
22) Disciplinary Record Documentation – relating to and disciplinary action taken against the member of staff. In accordance with the Trust’s Disciplinary Procedure records should be kept on individual’s Personal Files detailing the nature of any breach of discipline, the date, nature
and duration of action taken, its outcome and any subsequent developments. These records should be destroyed when the period of the warning has elapsed. Individuals have the right to confirm with their manager that this has taken place. Investigation files will be retained within Human Resources.

23) **Individual Performance Reviews/Appraisals/Personal Development Plans.**

24) **Study Leave Forms** or details of any training/development undertaken.

25) **Sickness Absence** – for the current year these may be held centrally but at the end of each year this should be transferred to the individual’s personal file. Documentation should include Return to Work Interviews. It should also include any information/correspondence received/obtained in connection with the individual’s health and/or sickness absence.

26) **Annual Leave** – for the current year these may be held centrally but at the end of each year this should be transferred to the individual’s Personal File and retained for 2 years.

27) **Other Leave** – Records of other leave, including special leave and/or maternity leave taken, including the relevant application forms and approval notification.

28) **Accident/Adverse Event Reports** – copies of any accidents or adverse events in which the individual has been involved during their employment.

29) **Grievance** - correspondence relating to grievances raised. Investigation files will be retained within Human Resources.

30) **Employment Termination Records** – Employee resignation letter and copy of their ESR termination form.