Standard Operating Procedure for Personal File Management

This standard operating procedure applies to all staff who have responsibility for the creation, maintenance and management of personal files.

Its purpose is to set out and promote a culture of good practice around the retention of information on personal files. This is to ensure that information is kept safe, secure and up to date.

This Standard Operating Procedure details the processes for the creation, maintenance and management of personal files.

This document should be read in conjunction with the Records Management Policy.

1. Recruitment Team Responsibilities

- Keep an accurate record of recruitment documentation for all successful candidates that join SHSC
- Ensure that documentation is collected as part of the pre-employment process in line with NHS Employers guidelines, as per the Recruitment and Selection Policy

2. Line Manager responsibilities

- Keep current and accurate records of documentation related to employees throughout their employment with SHSC
- Ensure all personal files are stored securely

3. Employees who commenced at SHSC post April 2020

The recruitment team will create an electronic Recruitment File which will be retained securely in HR. Line managers can request copies of the contents of this recruitment file by submitting a request by email to a member of the HR Advisory team or Recruitment Team Leader. The recruitment file will contain:

- Summary of selection form
- Application form
- Job Description and Person specification
- Advert text
- Conditional offer letter and email
- Copy of DBS
- Occupational health suitability report/consultation report
- ID
- Right to Work in the UK
- Proof of identity
- Proof of address
- Copies of qualification certificates (if applicable)
- Professional registration screenshot (if applicable)
- References
- Communication emails
- Inter Authority Transfer (IAT) (if applicable)
- New starter forms
- Final offer letter & contract

Line managers should create an electronic personal file to retain locally. It is important both for reasons of security and completeness, that all documents are saved in the file in a timely manner and labelled with employee name, file name and date. This minimises the chance of breaches of confidentiality and ensures that the file represents an up to date record of an individual's employment. The personal file should contain the following information:

- **Personal details**
  - Name, address, emergency contact numbers, national insurance number
  - Personal number
  - Driving licence details for nominated drivers
  - Post details change forms (ESR2PC)
  - Bank contract – if applicable
  - Induction record
  - Accident forms

- **Training**
  - Mandatory training (if not held electronically)
  - Other relevant training
  - Policy and procedures – record of those read, understood and signed

- **Line Management**
  - Supervision/PDR records (where they are not held on other electronic systems)
  - Disciplinary records – on expiry of disciplinary warnings, the letter should be removed from the personal file and destroyed
  - Grievance/Capability/Unacceptable behaviours formal outcome letters
  - Any other documents the line manager feels are relevant to the employee's employment

- **Attendance** *Full details should be removed from the file after 2 years with a condensed version retained on ESR*
  - Sickness – welcome back to work meetings, Occupational Health correspondence, fit notes
  - Leave – annual leave record, carer leave record, parental leave, study leave

- **General correspondence**

  This section is for individual line management judgement and can include applications for regrading, records of flexible working agreements.

4. Employees whose employment at SHSC began pre-April 2020

Line managers will have received a paper personal file from the recruitment team.

Line managers are responsible for ensuring personal information is kept secure, confidential and updated regularly as required.

It is at the discretion of the line manager if they wish to create an electronic or paper personal file, however it important to ensure this is consistent across the team to avoid duplication and gaps in information.

The information that should be retained in a personal file for these employees is as outlined above in Section 3.

5. Maintenance of personal files

It is important both for reasons of security and completeness, that all personal information on staff is filed away in consistently and in a timely manner. This minimises the chance of breaches of confidentiality and ensures that the file represents an up to date record of an individual’s employment.

Some information e.g. supervision and PDR records are held in electronic systems and further copies do not need to be saved. However, e-forms should be downloaded and saved/printed and held in the relevant personal file for audit purposes and confirmation of change authorisation.

6. File Security & Access

For security reasons paper personal files should be kept in lockable cabinets or drawers. Any files removed from the filing system should be returned as soon as possible. A filing system should be used that ensures when a file is removed from the system it can be easily located.

Electronic personal files should be saved in a restricted file when held in shared W Drive folders with limited access. It is not appropriate for electronic personal files to be saved in personal H drives. Folders with restricted access can be created by completing the Central Data Storage Access form on the IMST Self-Service Portal, stipulating the employees you wish to have access.

It is recognised that Directorates may choose to hold paper personal files at different ‘levels’ in the organisation, to respond to differing management arrangements, geographical spread, etc. It is important then that access to paper files should be properly controlled. Designated key holders should be clearly identified for each filing system, and ensure that any access is for *bona fide* reasons.

Staff have legal rights of access to their own personal files held by their employers. The Trust takes the view that a file should be made available if an individual makes a request. In such cases managers are advised to ensure the confidentiality of any references provided by a previous employer, which may be on the file is maintained. Such access to a personal file should be supervised by the manager responsible for the files.

Members of the HR Department may require access to personal files from time to time and will provide written confirmation of the request if asked to do so.

7. Transfer of personal files when staff move internally

When a member of staff moves location, Department or Directorate within the Trust, it is the responsibility of their existing manager to deliver the personal file to the new manager, immediately after the last working day of the member of staff concerned.

For paper personal files, signed confirmation of the safe receipt of the file should be obtained from the new manager and held for audit purposes. Where delivery by hand proves impossible, transport will arrange a special delivery of files to other work sites, confirmation of receipt should still be requested from the new (‘receiving’) manager.

If using the post, care should be taken when parcelling the file(s) to ensure that the parcel will remain secure during its journey.

Information relating to the new appointment/transfer of the member(s) of staff concerned will be sent retained by HR in a recruitment file, as outlined in section 3.

For electronic personal files, managers should ensure that they transfer the data in a secure way. Please contact the IT Service Desk for advice on how to achieve this safely. Email confirmation of receipt should be retained locally for audit purposes.

8. Personal file management on termination of an employee

The personal files of staff who have left the Trust should be delivered to the HR Department on the last day of employment, or as soon as possible thereafter. It is the responsibility of the line manager to ensure this occurs in a timely manner.

Where an employee has a recruitment file held in HR and a personal file (paper or electronic) with the line manager, these files will be combined into one record by the HR department.

Personal files must be retained for a period of 6 years after termination of employment or until the former employees reach 70 years of age, whichever is the later. HR will be responsible for the maintenance and security of a central store for the personal files of staff who have left the Trust. After the retention period has passed, the personal files will be destroyed and a summary of employment kept on ESR.