Shropshire Community Health NHS
NHS Trust

Policies, Procedures, Guidelines and Protocols

Document Details		
Title		**Management of Personal Files Policy**
Trust Ref No		1343-44964
Local Ref (optional)		Version 2.1
Main points the document covers		This policy enables all personal files to be compiled in a standard format and details the entitlement of staff in relation to their personal files.
Who is the document aimed at?		All staff with particular emphasis on managers who have line management responsibilities for staff
Owner		Human Resources
Approval process		
Who has been consulted in the development of this policy?		Managers, JNP, HR & Workforce Group
Approved by (Committee/Director)		HR & Workforce Group
Approval Date		7th July 2022
Initial Equality Impact Screening		Yes
Full Equality Impact Assessment		No
Lead Director		Director of Nursing and Allied Health Professionals Director for Infection Prevention
Category		Human Resources
Sub Category		None
Review date		3rd August 2024
Distribution		
Who the policy will be distributed to		All Staff
Method		Publication on Trust Intranet
Keywords		Personal files, retention, General Data Protection Regulation
Document Links		
Required by CQC		Yes
Other		None
Amendments History		
No	Date	Amendment
1	06/06/2011	Update due to organisational change (version 1)
2	15/11/2013	Reviewed by Human Resources and no changes required at this time. OD & Workforce Group agreed to extend next review date from 30/06/2012 to 30/06/2015
3	03/11/2014	Inclusion of Section 6 Data Protection Act compliance following advice from Information Commissioner's Office. Update to titles with regard to Directorate name and formatting to add paragraph numbers.
4	12/02/2015	Update to personal file checklist to include updated director posts checks
5	June 2018	3 yearly review of policy with the following amendments – policy name change, updated responsibilities for Managers,

		Recruitment Team, and Human Resources, new sections on definitions, General Data Protection Regulation, confidentiality, access to personal files, file notes, and archiving of personal files
6	June 2022 Version 2.1	Policy review – links to Staff Zone and names of policies updated. No other amendments made.

Contents

1 Introduction

1.1 This policy enables all personal files to be compiled in a standard format and details the entitlement of staff in relation to their personal files.

1.2 The storage, safe custody and access to personal files must be consistent throughout the Trust for employees to feel confident that we will meet our legal obligations and treat personal and sensitive information in a confidential and proper way.

2 Purpose and Scope

2.1 This policy is designed to:

- Provide guidance to managers on the contents of personal files.
- Provides guidance to managers so they can ensure personal files are kept safely and securely at all times.
- Provide guidance for everyone on appropriate access.
- Inform staff of the protocols that will apply to the safekeeping of their own personal file.

2.2 This process applies to all individuals employed by the organisation. It does not apply to external contractors or agency staff.

2.3 In implementing this policy, managers must ensure that all individuals are treated fairly and within the provisions and spirit of the Trust's Equality and Diversity (Everyone Counts) Policy.

3 Definitions

Word	Definition
Data Controller	The Trust is the data controller and must adhere to the six Data Protection Act principles for all personal data.
Data Subject	The data subject is the individual who is the subject of personal data.
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.
Retention	Retention is the period of time a document should be kept or retained in paper form.
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.

4 Responsibilities

4.1 Managers have a responsibility to ensure that:

- They comply with the requirements of this policy and related policies.
- The security of the personal file is maintained - files should be kept in a lockable cabinet, which is kept locked at all times when not in immediate use. Access by others should be limited to those with designated authority.
- Personal files are kept up to date and information contained is relevant.
- All paperwork should be secured within the file (i.e. no loose papers).
- Employees have access to their personal file on request through a Subject Access Request in line with the Information Governance Policy.
- Only one file should be held per individual.
- An indexing or tracking system is in place to ensure the manager has a file for every individual in their team and is able to track the whereabouts of any file that has been removed from the filing system temporarily or permanently.
- When a staff member moves department within the organisation, arrangements are in place to ensure the safe, secure transfer of their personal file to their new line manager. The new recruitment information (interview assessment sheets, pre-employment checks, conditional and unconditional letters etc.) should be incorporated into the existing file.
- When a staff member or bank worker leaves the Trust the personal file is transferred in a safe, secure manner to the Human Resources Department for archiving.
- Managers will not divulge any personal information about an individual to anyone in the Trust or external source other than for an employment reference, the management of an individual, a request from organisations where we have a statutory duty to supply information or where the individual has consented to the disclosure of the information to the person making the request.

4.2 Staff 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(s) of next of kin/emergency contact details
- Change in name
- Change in bank details
- Achievement of any professional qualifications
- Professional registration details
- Change in residency status

4.3 Recruitment Team are responsible for the completion and collation of the appropriate recruitment documentation which culminates in the creation of a personal file for new individuals to the Trust, or if an additional post, documentation to be added to the existing personal file. The personal file will be divided into the 7 sections outlined in Appendix 1 and the checklist should be kept at the front of the file.

4.4 Human Resources have a responsibility to provide advice in relation to the application of this policy and relevant employment law and best practice. In addition the HR team are responsible for the collation, archiving, indexing and retrieval of leaver's files.

5 Legislation

5.1 General Data Protection Regulation 2018

5.1.1 The General Data Protection Regulation (GDPR) applies from the 25 May 2018 and brings about a number of changes which impact on how we process, manage and store personal data. The GDPR, together with a new Data Protection Act 2018 replaces all pre-existing provisions under the Data Protection Act 1998.

5.1.2 The 8 principles under the Data Protection Act 1998 have been revised under the General Data Protection Regulation to 6 principles.

Personal data should be:

- Processed lawfully, fairly and in a transparent manner.
- Collected for specified, explicit and legitimate purposes.
- Adequate, relevant and limited to what is necessary.
- Accurate and where necessary kept up to date.
- Kept in a form which permits identification of data subject no longer than is necessary for the purposes for which those data are processed, and
- Processed in a manner that ensures appropriate security of the personal data.

Plus **Accountability** - Data controllers are responsible for compliance with the principles and must be able to demonstrate this to data subjects and the regulator.

6 Confidentiality

6.1 All the information contained within the personal file whether it is manual or computerised is treated as confidential. However, we have a statutory duty to supply legally required information to certain government agencies or departments such as the HM Revenue & Customs, Department of Work and Pensions, or the Police.

6.2 Other than where we are legally required to provide information (6.1) if an outside agency e.g. Bank or Building Society contact us for information the individual's written consent must be provided before the information is supplied.

7 Access to Personal Files

7.1 Only the following people should be granted access to individual personal files:

- The line manager or appropriate Head of Department
- Authorised administrators where there is a reason for access e.g. when filing information on the file.
- The Human Resources department
- Local Counter Fraud Specialist
- Internal or external auditors
- Employees can access their own personal file via a Subject Access Request (SAR).

7.2 Procedure for making a Subject Access Request

7.2.1 Under the General Data Protection Regulation and the Data Protection Act 2018 you can make a request to us regarding access, rectification, erasure, restriction and objection. Please refer to the Data Protection Policy for details on how to make a request, this can be verbal or in writing, and the Subject Access Form can be used to make your request.

7.2.2 It is the line manager's responsibility for ensuring any disclosure is compliant with data protection legislation, for example third party redaction, and managers should, where necessary, seek advice in the first instance from the Information Governance Lead.

7.2.3 The employee will be accompanied by their line manager or other appropriate manager during the viewing of their personal file. If the staff member wishes to be accompanied by their trade union representative when viewing their personal file then this will be accommodated, and the line manager or appropriate manager will also be present.

8 File Notes on Personal Files

8.1 From time to time it may be necessary for managers to make a file note regarding issues or concerns that have been raised with/by an individual. A file note should provide a balanced reflection of the issues discussed, any agreed actions, review dates, whether the issue is closed and the potential outcome if the issue is not resolved i.e. advice to be sought from the appropriate department, informal or formal processes to be implemented.

8.2 Individuals should be made aware that a file note is being made and that this is being placed on their personal file. The file note should be shared with the individual and if they wish to place their own comments on file to be read alongside the manager's file note then this should be done.

8.3 It is good practice for the individual to be asked if they wish to sign and date file notes and if they decline the manager should add a comment advising that the individual has been asked to sign but declined to sign the file note.

9 Retention, Archiving and Disposal of Personal File

9.1 Retention of Personal Files

9.1.1 Personal files will be kept until the employee's 75th birthday after which they will be confidentially destroyed in line with the Trust's Records, Retention, Archiving and Disposal Policy.

9.2 Archiving of Personal Files

9.2.1 From 1st October 2018 when an employee or bank worker leaves the Trust the personal file will need to be transferred to the Human Resources Department for archiving - this should be done within 5 working days of the individual's leaving date.

9.2.2 The Records and Document Management Policy provides guidance and advice in relation to safely transferring personal confidential data and records tracking.

9.2.3 Other types of staff record and exceptions to the general retention period are set out in the Trust's Records and Document Management Policy (guidance on based on Records Management - NHS Code of Practice).

10 Email Records

10.1 The Trust does not have a document management system in place to retrieve emails for a subject access request. In addition we are not the data controller for email sent via nhs.net and therefore we are unable to carry out searches on the information.

10.2 Consequently, managers must ensure that any important emails relating to an individual are printed off and a copy placed on the individual's primary record i.e. the personal file of the individual.

11 Related Documents

11.1 The following documents contain information that relates to this process and procedure:

- Equality and Diversity (Everyone Counts) Policy
- Data Protection Policy
- Records and Document Management Policy

12 Dissemination

12.1 This policy will be disseminated by the following methods:

- Executive Directors and Managers – to disseminate within their areas
- Published on the website
- Awareness raising by Human Resources and staff side representatives

13 Advice

13.1 Advice on this process and procedure should be sought in the first instance from HR.

14 Review and Compliance Monitoring

14.1 Review

This process and procedure will be periodically reviewed (at least every 3 years) in light of any developments in employment legislation or employee relations' practice and, if necessary, revised in order to ensure their continuing relevance and effectiveness.

14.2 Compliance Monitoring

The Human Resources team will monitor compliance with this policy by means of random personal file audits, or other appropriate compliance methods.

Appendix 1 Contents of a Personal File

Below is a checklist for the areas in which data should be held. The documentation identified should be held on every employee and is the minimum required. If managers find information is missing and cannot locate copies they should contact the HR department in the first instance.

This checklist should be kept at the front of the file. The front cover of a personal file should only record the employee's name and no other information.

Section 1: PERSONAL DETAILS	**On File**
First Name and Surname	
Date of Birth (verified)	
Employee Number	
Contact Details – address and telephone numbers should also be on ESR	
Next of Kin or Emergency Contact Details – should also be on ESR	

Section 2: CORRESPONDENCE	
This section would include any correspondence relating to the individual's employment.	

Section 3: GENERAL INFORMATION	**On File**
Old Annual Leave Records Leave entitlement for 2018 onwards should be recorded on Electronic Staff Record	
Confidentiality Form	
Copy of Driving Licence - photo card signed and dated to say original seen	
Copy of current insurance certificate and MOT certificate stating 'business use' cover, signed and dated to say originals seen	
Supervision or Meeting Notes	
Lease Car Documentation – if applicable	
Incident Forms – if applicable	
Induction Checklist – signed and dated	

Section 4: SICKNESS ABSENCE	
This section would include self-certification forms, GP Fit notes, return to work interviews, Occupational Health reports, managing attendance at work correspondence.	

Section 5: TRAINING AND APPRAISAL INFORMATION	**On file**
This section would include details of any training or development activities, study leave forms etc. Managers should keep paper copies of Personal Development Reviews (PDR) on file.	

Section 6: ASSIGNMENT INFORMATION	**On File**
Statement of Particulars – the employment 'contract' signed and dated by both employee and manager	
Starter Form – should be signed and dated by the employee and manager	
Any other ESR forms should be signed and dated by employee and Manager	
Section 7: RECRUITMENT – For <u>every</u> post held there should be …….	**On File**
Advertisement for the post that the individual was recruited from	
Job Description and Person Specification current and signed by both employee and line manager	
Application Form	
Interview Assessment Sheets - should be signed and dated by interviewers	
Conditional Job Offer Letter	
Acceptance of post form - signed and dated by individual	
Pre-Employment Checklist – signed and dated by Recruitment Team	
Proof of Identity - 2 address and 1 photo id OR 1 address and 2 photo id photocopy original documents signed and dated to say originals seen	
Right to Work in UK photocopy original documents, signed and dated to say originals seen	
Professional Registration Details evidence of current registration i.e. a print-out from the relevant website	
Copies of Qualifications relevant to the post as detailed in person specification, signed and dated to say originals seen	
References cover a minimum of 3 years employment and at least 2 previous employers	
Performers Lists & Healthcare Professional Alert Notice Web Check	
Occupational Health Clearance	
Disclosure and Barring Service Check (if applicable)	
Unconditional Job Offer Letter	
Director Posts Only:	
Search of insolvency and bankruptcy register	
Additional insolvency and bankruptcy	
Search of disqualified directors register	
Background check (including Google search)	
Declaration of fitness signed and dated	