Trust Policy

University Hospitals Plymouth NHS Trust

Employee Records Management

Issue Date	Review Date	Version
February 2015	**Extended to August 2022**	**4.2**

Purpose

The purpose of this policy is to provide clarification as to what information should be held by Plymouth Hospitals NHS Trust on future, current and past employees.

Who should read this document?

This policy relates to Agenda for Change and Medical and Dental applicants, current and past employees on substantive contracts.

Key Messages

As an employer the Trust has a responsibility under the Data Protection Act (1998) to ensure that all information held on its prospective, current and former staff is appropriate, not excessive, securely held, accessible and destroyed in a timely manner.

Core accountabilities	
Owner	HR Business Partner
Review	JSNC
Ratification	Director of People
Dissemination (Raising Awareness)	HR Business Partner
Compliance	HR Business Partner

Links to other policies and procedures

Sickness Absence Policy
Performance and Conduct Policy

Version History

1	November 2008	
2	February 2011	Review date extended to January 2012 by Martin Bamber
3	March 2011	Trust Commitment to Valuing People amended in line with the Equality Act 2010 Electronic policy paths updated
4	February 2015	Reviewed and Updated by HR Partner
4.1	June 2020	Extended to May 2021 by Lisa White
4.2	August 2021	Extension granted until August 2022

The Trust is committed to creating a fully inclusive and accessible service. Making equality and diversity an integral part of the business will enable us to enhance the services we deliver and better meet the needs of patients and staff. We will treat people with dignity and respect, promote

equality and diversity and eliminate all forms of discrimination, regardless of (but not limited to) age, disability, gender reassignment, race, religion or belief, sex, sexual orientation, marriage/civil partnership and pregnancy/maternity.

An electronic version of this document is available on Trust Documents. Larger text, Braille and Audio versions can be made available upon request.

Contents

1 Introduction

This document sets out the Trusts responsibilities in regard to employee files and records.

2 Purpose, including legal or regulatory background

The purpose of this policy is to provide clarification as to what information should be held by Plymouth Hospitals NHS Trust on future, current and past employees.

As an employer the Trust has a responsibility under the Data Protection Act (1998) to ensure that all information held on its prospective, current and former staff is appropriate, not excessive, securely held, accessible and destroyed in a timely manner.

The storage, safe custody and access to personal files/records must be consistent throughout the Trust for applicants and past and present employees to feel confident the Trust will meet its legal obligations and treat personal and sensitive information in a confidential and proper way.

3 Principles

The HR Records Management Policy and Procedure is based on the following principles:

- The Trust recognises that accurate and managed employee records are essential to support the operational work of the Trust.
- The Trust recognises its responsibilities in relation to keeping appropriate records for appropriate timescales.
- The Trust will use electronic methods of storage wherever possible as it is recognised this offers the most cost effective and efficient method of record storage.
- The Trust will hold personal records in line with the Records Management; NHS Code of Practice, based on current legal requirements (the eight principles of the Data Protection Act.) and professional best practice.
- The Trust recognises that the best way of holding and managing records in line with operational and legal requirements is to actively work towards the creation of a single Personal Employment Record (PER) for each employee.

4 Duties

The **Chief Executive and the Trust Board** have a legal responsibility to oversee this Policy and to ensure its correct application.

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.

The **Human Resources Department** will also manage any Service Level Agreements (SLA's) relating to the management of employee records.

Every **Manager** is responsible for ensuring that:

- The employee records they hold are kept securely and the contents of files are in line with the requirements of this policy.
- Where separate working files are held, information is transferred to the Personal Employment Record (PER) or destroyed at regular intervals in line the NHS Records Management: Codes of Practice - 2006.
- Where separate working files are not held, records should be filed together in a logical order.
- Staff have access to the records held about them, on request in writing.
- Terminated files should be sent to the HR Department for secure archiving.
- The security and traceability of the Personal Employment Record / working file is maintained.

- PER's and working files for transferring staff should be sent to the HR Department on receipt of the letter of resignation.
- Advice is sought from the HR Department if they are unsure about the practical application of this policy**.**
- Every member of staff is responsible for informing both their Manager and the Workforce Development Team in writing 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.
    - Professional Registration details.

Every member of the **Recruitment and Resourcing** team will be responsible for:

- Creating an accurate Personal Employment Record for each new starter and updating the PER for staff transfers.
- Sending PERs to HR Central filing store on completion of pre-employment checks of staff commencing in post or transfer within Trust.

5 Key elements

TYPES OF EMPLOYEE RECORDS

Pre-employment – Vacancy File

All documentation in support of a recruitment process will be collated and retained by the Recruitment and Resourcing Team under the job reference associated with the process.

A vacancy file will contain records such as vacancy details and approvals, the shortlisting and interview documentation of unsuccessful applicants and the eventual selection decision.

The vacancy file is held by the Recruitment and Resourcing Team for a period of twelve months from the date of interview.

All documentation for successful applicants is transferred from the vacancy file to the PER.

Personal Employment Record (PER) – HR File

A personal employment record is a file containing key documents relating to an individual's employment history with the Trust. It includes items such as decisions about recruitment, pay, training, promotion, transfer, disciplinary action or dismissal.

PERs are predominantly held in the central HR filing system, but can on agreement by the HR Department, be held locally be a line manager.

Local/Line Managers File – Working File

A working file is a collection of personal data relating to an individual and stored locally in the department, which contains information needed for the day to day management of an individual.

Where necessary, a manager may store informal file notes regarding the employee's conduct or performance.

File notes should be shared with the employee and where possible signed by both parties. File notes should only relate to professional matters.

ESR Record

The Trust uses the national Electronic Staff Record to hold summary information regarding employees. ESR is also the core data source for other HR related systems which hold personal data. Those systems include:-

- E-Appraisal system (Appraisal & competencies).
- OLM (Learning Management System for all L&D activities).
- Health Rostering System (Rostering and Time and Attendance).
- RA (Clinical and IT system access / safe recruitment).
- Intrepid (Junior Doctors Training Administration System).

Terminated File

When an employee leaves the organisation, the working file should be sent to the HR department for amalgamation with the PER.

A Terminated file is retained for 6 years after the individual leaves employment with the Trust and is a reduced version of the Personal Employment Record. It will only contain essential information for 30 years or until the individual's 70th birthday, whichever is the latter.

The terminated file will be stored in the central HR filing system.

Training Files

The Trust is working towards a position where all training records will be electronically stored on the OLM system. Where paper training records are still in use, these must be filed in the PER upon completion of the course.

RETENTION AND DISPOSAL SCHEDULES

Retention and disposal schedules are clearly set out in Appendix 3**.** Managers who hold files on their own employees should robustly adhere to this schedule in line with legal requirements. On the termination of employment, the manager must send any file relating to the outgoing member of staff to the HR department to be updated and archived and eventually destroyed in line with Appendix 3. Minimum retention periods are to be calculated from the beginning of the year after the last date on the record.

HR PROCEDURAL RECORDS

At the end of any formal HR management proceedings, an outcome letter will be issued and a copy will be placed on the individual's PER. The outcome letter must include (if a disciplinary matter) the duration of any warning given. If the warning follows on from a previous live warning, then both warnings should be kept filed within the PER.

The HR Department will keep a central secure storage system for formal disciplinary and grievance matters, in which all documentation relevant to the matter will be held. This will usually consist of the management pack for a formal process and any other information that was fundamental to the Trust reaching the outcome it did. Additionally, a summary record will be updated on ESR against the individual's name.

Upon expiry, the warning will be transferred from the working file to the PER, clearly marked “expired”.

Access and Use of Expired HR Management Records

Records stored as described will provide the safeguards the Trust needs to manage potential legal risk. It will also ensure that out of date and extraneous information is not taken into account in an irrelevant manner, in terms of other employment decisions / references.

The Trust commits to these records being used in the following situations:

- For cases which proceed to an Employment Tribunal.
- For cases of litigation – claims for personal damages etc.
- For matters involving the police or other professional bodies, which require the disclosure of such matters for a reasonable purpose.
- For matters involving multi-agency information sharing; specifically Safeguarding of Children and Vulnerable Adults procedures.

These records will not be made available to managers who are simply curious to know the previous history of staff they now employ.

The Director of HR / Deputy Director of HR will be responsible for ensuring that the record is only released in line with the specific reasons stated above. Authorisation will also need to be obtained from the Director of HR / Deputy Director of HR for the release of any record.

The HR department will keep such information for 6 years post the individual leaving employment and then will securely destroy the record with a summary retained by HR for 30 years or until the individual’s 70th birthday, whichever is the latter.

Attendance Processes

The Trust will use sickness records for a number of reasons; to evaluate an employee’s ability, to make reasonable adjustments and to fulfil Health and Safety obligations. Records which detail specific information about the employee’s illness / injury should be held separately from absence records, which purely record when an individual attended.

REQUESTS TO SEE FILES

Access to files should be provided on a strictly need to know basis. Data controllers should satisfy themselves that any third party requesting access to records has a legitimate right of access.

Management requests to see Personal Employment Records (PERs)

There will be times when Managers or HR Representatives will need to access the PER of an individual that they do not hold a file for.

Requests for access to the PER should be made in writing to the HR Administration Team who will keep an electronic record of the file removal from the HR Central store.

When in possession of the PER, the Manager / HR Representative takes responsibility for the record and may be held accountable under the Trust’s Disciplinary policy for any loss. The Manager will ensure that the record is held securely.

Both HR and the manager have a responsibility to record the whereabouts of the file, including the name of the person it has been released to and the date it was dispatched/received.

Employee Access to Records held about them.

Any employee may request to see the personal data held on them by the Trust. They should write to their line manager, specifying the records they wish to see.

The manager will request the PER in writing via the HR Administration Team. A file must never be released to an individual, only to a manager with line management responsibility for the individual or a HR representative.

The manager must take responsibility for providing the employee with all the records they have asked for.

If the request is from an ex-employee, then the Trust will charge £50 to cover the administration of this service.

Requests to see Vacancy Files

Unsuccessful candidates / applicants may also request in writing to see data held about them in relation to a recruitment process. The applicant will not be able to access the application forms of other candidates but should be able to see the shortlisting information and the scoring sheets from the interview process.

REQUESTS TO SEE EMPLOYMENT REFERENCES

Employees may request, in writing, to see references provided by former employers both internal and external. If a referee has indicated they wish a reference to remain confidential, steps will be taken to anonymise the reference and the referee will be contacted to make them aware the content is going to be shared. The employee will be referred back to the referee for queries relating to the reference provided.

6 Overall Responsibility for the Document

The HR Director is responsible for ratifying this document. The HR Business Partner has the responsibility for the dissemination, implementation and review of this policy.

7 Consultation and Ratification

The design and process of review and revision of this policy will comply with The Development and Management of Trust Wide Documents.

The review period for this document is set as default of five years from the date it was last ratified, or earlier if developments within or external to the Trust indicate the need for a significant revision to the procedures described.

This document will be approved by the JSNC and ratified by the Director of HR &OD.

Non-significant amendments to this document may be made, under delegated authority from the Director of HR & OD, by the nominated author. These must be ratified by the Director of HR & OD and should be reported, retrospectively, to the approving JSNC.

Significant reviews and revisions to this document will include a consultation with named groups, or grades across the Trust. For non-significant amendments, informal consultation will be restricted to named groups, or grades that are directly affected by the proposed changes.

8 Dissemination and Implementation

Following approval and ratification, this policy will be published in the Trust's formal documents library and all staff will be notified through the Trust's normal notification process.

Document control arrangements will be in accordance with The Development and Management of Trust Wide Documents.

The document author(s) will be responsible for agreeing the training requirements associated with the newly ratified document with the named Heinz Scheffer and for working with the Trust's training function, if required, to arrange for the required training to be delivered.

9 Monitoring Compliance and Effectiveness

The Trust will undertake regular audit of the processes specified in this policy. It should be noted that the responsibilities in this policy are legally enforceable and that managers failing to uphold their responsibilities may find themselves in breach of internal disciplinary policies and legislation.

10 References and Associated Documentation

List main references, for example:

- Key legislation
- Department of Health regulations and guidelines
- Other Governmental regulations and guidelines
- Regulatory agency (eg HSE, NPSA, NICE) regulations and guidelines
- Professional group rules, regulations and guidelines
- Accreditation and compliance assessments

Dissemination Plan and Review Checklist | Appendix 1

Dissemination Plan	
Document Title	Employee Records Management
Date Finalised	February 2015
Previous Documents	
Action to retrieve old copies	

Dissemination Plan

Recipient(s)	When	How	Responsibility
All Trust staff		Information Governance StaffNet Page	Information Governance Team

Review Checklist		
Title	Is the title clear and unambiguous?	Yes
	Is it clear whether the document is a policy, procedure, protocol, framework, APN or SOP?	Yes
	Does the style & format comply?	Yes
Rationale	Are reasons for development of the document stated?	Yes
Development Process	Is the method described in brief?	Yes
	Are people involved in the development identified?	Yes
	Has a reasonable attempt has been made to ensure relevant expertise has been used?	Yes
	Is there evidence of consultation with stakeholders and users?	Yes
Content	Is the objective of the document clear?	Yes
	Is the target population clear and unambiguous?	Yes
	Are the intended outcomes described?	Yes
	Are the statements clear and unambiguous?	Yes
Evidence Base	Is the type of evidence to support the document identified explicitly?	Yes
	Are key references cited and in full?	Yes
	Are supporting documents referenced?	Yes
Approval	Does the document identify which committee/group will review it?	Yes
	If appropriate have the joint Human Resources/staff side committee (or equivalent) approved the document?	Yes
	Does the document identify which Executive Director will ratify it?	Yes
Dissemination & Implementation	Is there an outline/plan to identify how this will be done?	Yes
	Does the plan include the necessary training/support to ensure compliance?	Yes
Document Control	Does the document identify where it will be held?	Yes
	Have archiving arrangements for superseded documents been addressed?	Yes
Monitoring Compliance & Effectiveness	Are there measurable standards or KPIs to support the monitoring of compliance with and effectiveness of the document?	Yes
	Is there a plan to review or audit compliance with the document?	Yes
Review Date	Is the review date identified?	Yes
	Is the frequency of review identified? If so is it acceptable?	Yes
Overall Responsibility	Is it clear who will be responsible for co-ordinating the dissemination, implementation and review of the document?	Yes

Equalities and Human Rights Impact Assessment | Appendix 2

Core Information	
Date	February 2015
Title	Employee Records Management
What are the aims, objectives & projected outcomes?	The document does not require an EIA
Scope of the assessment	
Collecting data	
Race	
Religion	
Disability	
Sex	
Gender Identity	
Sexual Orientation	
Age	
Socio-Economic	
Human Rights	
What are the overall trends/patterns in the above data?	
Specific issues and data gaps that may need to be addressed through consultation or further research	

Involving and consulting stakeholders	
Internal involvement and consultation	
External involvement and consultation	
Impact Assessment	
Overall assessment and analysis of the evidence	

Action Plan				
Action	Owner	Risks	Completion Date	Progress update

Appendix 3	Retention & Disposal Schedule			
TYPE / SUBTYPE OF RECORD	**DERIVATION**	**TRUST RETENTION PERIOD**	**FINAL ACTION**	**LOCATION**
Clinical training records / student files	Records Management: NHS Code of Practice	30 years	Destroy under confidential conditions	Training / PER
Consultants records relating to the recruitment of	Records Management: NHS Code of Practice	5 years	Destroy under confidential conditions	PER / ESR
CVs for non-executive directors (successful applicants)	Records Management: NHS Code of Practice	5 years following term of office	Destroy under confidential conditions	PER
CVs for non-executive directors (unsuccessful applicants)	Records Management: NHS Code of Practice	2 years for shortlisted candidates	Destroy under confidential conditions	Vacancy file
Disclosure & Barring Service (DBS) Clearance	DBS Code of Practice	6 months from recruitment decision	Destroy under confidential conditions	DBS Lead
Duty rosters	Records Management: NHS Code of Practice	4 years after the year to which they relate	Destroy under confidential conditions	Trust-wide
Employment relations (not routine staff matters), including employment tribunals	Records Management: NHS Code of Practice	10 years	Destroy under confidential conditions	HR Director's office
Timesheets for individual members of staff including locum doctors (personal record of hours actually worked)	Records Management: NHS Code of Practice	2 years after the date to which they relate Locum (team based) timesheets – 6 months where a master copy held centrally.	Destroy	Working Files
Health and safety documentation	Records Management: NHS Code of Practice	3 years	Destroy under confidential conditions	Health & Safety office
HR Management files / investigation reports	The Information Commissioner Code of Practice	6 years and a summary to be retained for 30 years or until individual's 70th birthday, whichever is the latter	Destroy under confidential conditions	HR Operational Team base
Incident forms - accidents, injuries, diseases and dangerous occurrences	Records Management: NHS Code of Practice	8 years	Destroy under confidential conditions	Datex / PER / ESR
Job advertisements	Records Management: NHS Code of Practice	Templates held indefinitely to assist with future recruitment campaigns	N/A	PER / Vacancy File

Job applications (unsuccessful)	Records Management: NHS Code of Practice	1 year	Destroy under confidential conditions	ESR / Vacancy File
Job applications (successful)	Records Management: NHS Code of Practice	6 years after individual leaves service	Destroy under confidential conditions	PER

TYPE/SUBTYPE OF RECORD	DERIVATION	TRUST RETENTION PERIOD	FINAL ACTION	LOCATION
Job descriptions	Records Management: NHS Code of Practice	6 years after individual leaves service	Destroy under confidential conditions	PER / Vacancy File
Leavers' dossiers	Records Management: NHS Code of Practice	6 years after individual leaves service Summary to be retained for 30 years or until individual's 70th birthday, whichever is the latter	Destroy under confidential conditions	PER
Meetings and minute papers of major committees and sub-committees	Records Management: NHS Code of Practice	30 years	Destroy under confidential conditions	HR Director's office
PERSONAL EMPLOYMENT RECORD (PER) See 'Guidance on the Contents of Employee Files - Section 5	Records Management: NHS Code of Practice	6 years after individual leaves service, at which time a summary of the file must be kept for 30 years or until the individual's 70th birthday, whichever is the latter	Destroy under confidential conditions	PER / E-Appraisal / ESR
WORKING FILES See 'Guidance on the Contents of Employee Files - Section 5'	Records Management: NHS Code of Practice	2 years	Destroy under confidential conditions	Working File
Records relating to events notifiable under the Retirement Benefits Schemes (Information Powers) Regulations 1995, records concerning decisions to allow retirement due to incapacity, pension accounts and associated documents	The Retirement Benefits Schemes (Information Powers) Regulations 1995	6 years after individual leaves service, at which time a summary of the file must be kept until the individual's 70th birthday, whichever is the latter	Destroy under confidential conditions	PER / Payroll / Occupational Health
Recruitment / Vacancy requisitions	Local	18 months	Destroy under confidential conditions	Recruitment Dept.

TYPE/SUBTYPE OF RECORD	DERIVATION	TRUST RETENTION PERIOD	FINAL ACTION	LOCATION

(Recruitment) **VACANCY FILES** See 'Guidance on the Contents of Employee Files - Section 5'	Local The Data Protection Act 1998 (As amended)	12 months from date of interview (Certain exceptions apply to Consultants, EDs and NEDs – see above)	Destroy under confidential conditions	Vacancy File
(Recruitment) **VACANCY FILES** See 'Guidance on the Contents of Employee Files - Section 5'	Local The Data Protection Act 1998 (As amended)	12 months from date of interview (Certain exceptions apply to Consultants, EDs and NEDs – see above)	Destroy under confidential conditions	Vacancy File
Study leave applications	Records Management: NHS Code of Practice	5 years from date of request	Destroy under confidential conditions	PER
Subject access requests under DPA (records of requests)	Records Management: NHS Code of Practice	3 years after last action	Destroy under confidential conditions	Central Records
Training Plans	Records Management: NHS Code of Practice	2 years	Destroy under confidential conditions	Training Dept.