

## Records management policy

Board library reference	Document author	Assured by	Review cycle
P017	Head of Compliance	Audit and Risk Committee	3 Years

This document is version controlled. The master copy is on Ourspace.

Once printed, this document could become out of date.

Check Ourspace for the latest version.

## Contents

- 1. Introduction.....3**
- 2. Purpose or aim.....3**
- 3. Scope .....3**
- 4. Policy statement .....3**
  - 4.1 Retention and disposal schedules..... 3
  - 4.2 Paper documents ..... 3
  - 4.3 Workgroups..... 4
  - 4.4 Files and data management standards ..... 4
- 5. Training.....4**
- 6. Roles and responsibilities .....4**
  - 6.1 The Chief Executive ..... 4
  - 6.2 The Senior Information Risk Owner (SIRO) ..... 4
  - 6.3 Executive Directors and Local Delivery Unit Directors ..... 4
  - 6.4 Integrated Governance Group ..... 4
  - 6.5 Head of Compliance ..... 4
  - 6.6 All Users of AWP ICT Systems..... 4
- 7. Implementation .....5**
- 8. Standards .....5**

Records management policy

9. Monitoring and audit .....5

10. Archiving of master documents.....5

11. References .....5

## 1. Introduction

As a public body we are required by law to manage our records properly. Legislation such as the General Data Protection Regulations 2018 and Freedom of Information Act 2000 set out specific requirements in relation to the creation and management of records.

## 2. Purpose or aim

Records management is vital to the delivery of our services in an orderly, efficient, and accountable manner. Effective records management will help ensure that we have the right information at the right time to make the right decisions; this policy provides a baseline framework of standards and practices for the management of records.

## 3. Scope

This is a Trust-wide Policy and applies to all staff and personnel operating under the auspices of the Trust, including employees, locums, contractors, temporary staff, students, service user representatives, volunteers and partner agency staff.

This Policy applies to the three identified types of information processed, transmitted and maintained by the Trust. These are:

- Health and Social Care records (“clinical” records about service users and carers)
- Staff records (“corporate” records about staff)
- Management records (“corporate” records about the Trust)

Due to the integration in Health & Social Care Teams of staff from partner organisations there may be additional “data controllers” interested in the content of the single Health & Social Care Record of which the Trust is the data controller.

Where a third party has an organisational policy that differs from this Policy, a formal agreement as to which policy statement applies shall be outlined and agreed in an appropriate protocol if necessary. In the absence of such an agreement, this Policy shall be deemed to have precedence.

## 4. Policy statement

The Trust shall implement appropriate systems and practices for the management of each type of information to ensure that the Trust’s Business Records document the Trust’s activities and that information can be identified and retrieved when required.

The Trust mandates the use of consistent standards for strategies, policies, standard operating procedures and associated documents, which can be found in the document development and management policy and associated document development handbook. (put in hyperlinks once approved and uploaded).

### 4.1 Retention and disposal schedules

It is a requirement that all Trust records are retained for a minimum period of time for legal, operational and safety reasons. The length of time for retaining records will depend on the type of record and its relation to the Trust’s functions.

The Trust has adopted the retention periods set out in the [Information Governance Alliance records management code of practice for health and social care 2016](#) available on the Department of Health Website.

### 4.2 Paper documents

Paper (non-clinical) documents should be considered either as uncontrolled versions of electronic documents or where a paper document is identified as a record it must be scanned into the relevant OurSpace Library for appropriate record management. Once transferred to OurSpace, the paper version must be securely destroyed unless there is a legal reason for its retention in accordance with Retention and Disposal Schedules.

### **4.3 Workgroups**

Existing document repositories on network workgroups (shared drives) shall be migrated to the relevant OurSpace Library according to business priority.

### **4.4 Files and data management standards**

The Trust has documented [files and data management standards](#) which should be adopted for corporate records.

## **5. Training**

All relevant Trust staff shall be made aware of their responsibilities for record-keeping and record management through formal induction as well as local induction and ongoing on the job training.

## **6. Roles and responsibilities**

### **6.1 The Chief Executive**

The Chief Executive is responsible for ensuring the Trust's compliance with applicable legislation and regulation.

### **6.2 The Senior Information Risk Owner (SIRO)**

The Executive Director of Finance and Commerce and Deputy Chief Executive shall be the Trust Senior Information Risk Owner (SIRO) and shall represent any relevant information risk to the Board of Directors.

### **6.3 Executive Directors and Local Delivery Unit Directors**

Executive Directors and Local Delivery Unit Directors are responsible for compliance with the records management standards specified in this policy within their directorates and local delivery units.

### **6.4 Integrated Governance Group**

The Integrated Governance Group shall monitor and report on the implementation of the Trust's Information Governance Management System.

### **6.5 Head of Compliance**

Compliance with this policy shall be monitored by the Head of Compliance, reporting to the Integrated Governance Group.

### **6.6 All Users of AWP ICT Systems**

All users of AWP Information and Communications Technology systems are responsible for ensuring that their use of these systems is conducted in compliance with this policy.

## 7. Implementation

An alert notifying staff of the change to this policy shall be issued using the Trust's standard policy alert system.

Implementation of the policy in practice shall be conducted by managers with responsibility for ensuring compliance.

This Policy shall be published in the Board Policy Library on OurSpace.

## 8. Standards

The following standards apply:

- The Records Management NHS Code of Practice,
- The Public Records Act 1958,
- The General Data Protection Regulations 2018,
- The Freedom of Information Act 2000,
- The Common Law Duty of Confidentiality,
- The Confidentiality NHS Code of Practice,
- The NHS Information Governance Guidance on Legal and Professional Obligations,
- Information Security Management NHS Code of Practice, and
- Any new legislation affecting records management as it arises.

## 9. Monitoring and audit

Compliance with this policy shall be monitored by the Head of Compliance, reporting to the Integrated Governance Group.

## 10. Archiving of master documents

The Board Policy Document Library on OurSpace is the only recognised repository for master versions of policy documents. Copies of this document must therefore not be stored elsewhere on the system, e.g. in workgroups.

The OurSpace document library system shall provide records management functionality to allow for the retrieval of previous versions of policy documents for audit purposes.

## 11. References

- General Data Protection Regulations 2018
- Freedom of Information Act 2000
- Computer Misuse Act 1990
- The Caldicott Report 1998
- NHS Information Security Management: Code of Practice
- NHS Confidentiality: Code of Conduct
- NHS Records Management: Code of Practice
- The International Standards for Information Security Management
- Health & Social Care Records Policy

## Records management policy

- Model Action Plan for Developing Records Management Compliant with The Lord Chancellor's Code of Practice under Section 46 of The Freedom of Information Act 2000
- A full list of the applicable legislation referenced in the compilation of this policy can be viewed in the [NHS Information Governance Guidance on Legal and Professional Obligations](#)

<b>Version History</b>				
<b>Version</b>	<b>Date</b>	<b>Revision description</b>	<b>Editor</b>	<b>Status</b>
1.0	14/01/2004	Version 1 Approved by IM&T Steering Group	Head of IM&T	Approved
2.0	26/03/2008	Approved by the Board of Directors	Information Governance Manager	Approved
3.0	01/12/2009	Approved by Quality and Healthcare Governance Committee	Information Governance Manager	Approved
4.0	18/03/2013	Approved Finance and Planning Committee	Information Governance Manager	Approved
5.0	15/04/2016	Approved Audit and Risk Committee	Head of Compliance	Approved
6.0	15/03/2017	Addition of procedures for records management	Head of Compliance	Approved
6.1	11/10/2018	Minor admin amendments (GDPR)	Co Sec	Approved