NHS

Kent and Medway

NHS and Social Care Partnership Trust

Overarching Records Management Policy

Document Reference No.	KMPT.InfoG.078.02
Replacing document	KMPT.InfoG.078.01
Target audience	Trust wide
Author	Head of Information Governance and Records Management
Group responsible for developing document	Information Governance Group
Status	Ratified
Authorised/Ratified By	Information Governance Group
Authorised/Ratified On	September 2023
Date of Implementation	September 2023
Review Date	September 2024
Review	This document will be reviewed prior to review date if a legislative change or other event otherwise dictates.
Distribution date	September 2024
Number of Pages	32
Contact Point for Queries	kmpt.policies@nhs.net
Copyright	Kent and Medway NHS and Social Care Partnership Trust 2023

DOCUMENT TRACKING SHEET

Overarching Records Management Policy

Version	Status	Date	Issued to/approved by	Comments
V0.1	Draft	January 2023		Merge of health and social care and corporate records management policies and procedures into one overarching document.
V1.0	Final	March 2023	Information Governance Group	Approved for use
V1.1	Draft	Sept 2023		
V2.0	Final	Sept 2023	Information Governance Group	Approved for use

REFERENCES

NHSX Records Management Code of Practice 2021
UK GDPR and Data Protection Act 2018
NHSE Data Security and Protection Toolkit (DSPT)
Professional Records Standards Body (PRSB)
Freedom of Information Act 2000 – specifically the Code of Practice - Section 46
Public Records Act 1958
Local Government Act 1972 – specifically Section 224
Health and Social Care Act 2008 – specifically Regulation 17
Limitation Act 1980

RELATED POLICIES/PROCEDURES/protocols/forms/leaflets

Records Retention and Destruction Policy	
Document Scanning Policy and Procedure	
Overarching Information Governance Policy	
Information Security Policy	
Data Quality Policy	
ICT Acceptable Use Policy	

SUMMARY OF CHANGES

Date	Author	Page	Changes (brief summary)
Jan 2023	Deputy Head of Information Governance and Records Management	Whole Policy	Merge of health and social care and corporate records management policies and procedures into one overarching document.
Sept 2023	Deputy Head of Information Governance and	Page 10 Para. 5 Page 11	Addition of direction around the uploading of psychological testing – raw data papers to Rio.

	Records Management	10.1.6	
June 2024	Deputy Head of Information Governance and Records Management	Page 29	Specific instruction added relating to admin staff writing into progress notes on behalf of registered clinicians.

CONTENTS

1 INTRODUCTION

1.1 This policy applies to all NHS records this includes all clinical and corporate records held in any format.

This policy applies to records of NHS patients treated on behalf of the NHS in the private healthcare sector and public health records and Adult Social Care records where these are integrated with NHS patient records.

All NHS records are Public Records under the Public Records Act 1958 S.3 (1)-(2). The Trust will take actions as necessary to comply with the legal and professional obligations set out in the NHSX Records Management Code of Practice 2021, in particular:

- Public Records Act 1958
- Data Protection Act 2018
- General Data Protection Regulations 2016
- Freedom of Information Act 2000
- Common Law Duty of Confidentiality
- NHS Confidentiality Code of Practice
- Lord Chancellors Code of Practice for Records Management.

and any new legislation affecting records management as it arises.

2 WHO DOES THIS POLICY APPLY TO?

2.1 This policy applies to all locum, permanent and fixed term contract employees (including apprentices) who hold a contract of employment or engagement with the Trust, and secondees (including students), bank, volunteers (including Associate Hospital Managers) and Non-Executive Directors. It also applies to external contractors, Agency workers and other workers who are assigned to Kent and Medway NHS and Social Care Partnership Trust.

3 PURPOSE

3.1 The primary function of the Policy is to provide a framework for the regular assessment of the Trust wide current state of record keeping and develop a consistent and effective records management programme to enable the improvement and development of record keeping.

3.2 The Trust's records are its clinical and corporate memory, providing evidence of action and decisions and representing a vital asset to support daily functions and operations. Records support policy formation, managerial decision-making and protects the interests of the public. They support consistency, continuity, efficiency and productivity and help deliver services in consistent, safe, appropriate and equitable ways.

3.3 To ensure from the moment a record is created until its ultimate disposal that the organisation:

- Controls both the quality and quantity of information it generates
- Complies with national record keeping standards, guidance and best practice
- Maintains all information in a manner that effectively services the needs of the Trust and those of its stakeholders

- Holds information securely
- Disposes of information securely and efficiently when it reaches the end of the retention period.

3.4 To ensure mandatory Trust wide training of data protection, security and confidentiality (including access to and the sharing of information) and the Freedom of Information Act 2000.

4 DUTIES

4.1 Chief Executive

The Chief Executive has overall responsibility for records management within the Trust. They are responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity. Records management is fundamental to this as it will ensure appropriate, accurate information is available as required.

4.2 Caldicott Guardian

The Trusts Caldicott Guardian is the Executive Medical Director, and has a particular responsibility for reflecting patients' interests regarding the use of patient identifiable information. They are responsible for ensuring patient identifiable information is shared in an appropriate and secure manner. They are the final reviewer for decisions relating to the handling, storage and disclosure of patient identifiable information and in the retention and destruction of all health records. Their explicit agreement is required prior to the destruction of any health record.

4.3 Senior Information Risk Owner

The Trusts Senior Information Risk Owner is the Executive Director of Finance and Performance, and has been allocated with lead responsibility for the Trust's information risks and provides a focus for the management of information risk at Board Level. The SIRO oversees the appropriate management of all information assets and provides a focal point for managing all information risks and incidents.

4.4 Data Protection Officer

The Trusts Data Protection Officer is the Head of Information Governance and Records Management, and has operational responsibility for the Records Management Policy and is responsible for the overall development and maintenance of the Records Management Policy and for ensuring it complies with legal and regulatory requirements. They are also responsible for providing learning and development with key learning points and for monitoring compliance to assess its overall effectiveness and will also give advice and guidance to inform staff of their obligations.

4.5 Locality Directors/Clinical Directors/Heads of Service/Department Managers

Locality Directors/Clinical Directors/Service Manager/Department Managers are responsible for ensuring the standard of local record keeping is in line with expectations of the organisation and professional bodies. They must also ensure that their locality and department records comply with the requirements of the organisations record keeping policies and procedures, and that those records are securely stored, audited and disposed of and a suitable documented record is maintained. They are also responsible for ensuring that their staff, including bank or agency staff are trained in and comply with these requirements. Service/Department managers are responsible for the development and monitoring of local procedures and protocols (SOPS) for the management of confidential data by staff.

4.6 **All staff**

All Trust staff are responsible for ensuring they comply with this policy and local guidance where this exists. Staff are also directed by their professional codes of practice which may also include guidance on record keeping. Staff must report all incidents involving records via the incident reporting system. This includes the loss of or missing records.

Everyone working for the NHS who handles' stores or otherwise comes across patient or person identifiable information has a common law duty of confidence to patients/individuals and to KMPT.

4.7 **Information Governance Group**

Will approve guidance and procedures related to records management. This is the sub-group with delegated duties to deal with information governance and overall records management issues and reports to the Audit and Risk Committee.

The Trust is subject to a number of legal, statutory and good practice guidance requirements covering records.

All staff members, volunteers and persons acting on behalf of the Trust

- All employees have a responsibility for any records they create or use. Any records created by an NHS employee are public records and may be subject to both legal and professional obligations.
- Staff must attend relevant training covering records management.
- Staff must refer any concerns and incidents to their manager.
- This responsibility will be set out in all job descriptions.

5 SCOPE

5.1 This policy applies to all KMPT staff irrespective of method of employment. A record is anything which contains information (in any media) which has been created or gathered as a result of any aspect of the work of the NHS employees, including consultants, agency, volunteers, students or bank staff. This guidance applies to any material which holds information gathered, including all computer databases, electronic and paper-based records, imaging, photographs, tapes, cassettes, CD's. emails etc. Records include all administrative records (e.g. personnel, estates, financial and accounting, notes associated with complaints) and all patient health records for all care groups across KMPT.

6 DEFINITIONS

6.1 **Health Record** – Section 205 of the Data protection Act 2018 (DPA18) defines a health record as a record which:

- Consists of data concerning health
- Has been made by or on behalf of a health professional in connection with the diagnosis, care or treatment of the individual to whom the data relates.

6.2 **Paper Records** – are records in the form of files, volumes, folders, bundles, maps, plans, charts etc.

6.3 **Electronic Records include the following examples:**

- NHS patient health records; Rio and PADS.
- NHS staff records; Electronic Staff Record (ESR).

- Digital Images stored within patient health record.
- CD-ROM/DVD or other storage media such as hard drives and servers.
- Emails
- Scanned records
- Text messages (both outgoing from the NHS and incoming from the patient)

6.3 **The National Archives** are the body that is responsible for advising on the management of all types of public records, including NHS records.

6.4 **Person identifiable information** would be any information that includes names, addresses, dates of birth, conditions etc. Whether electronic or manual records or record systems holding person identifiable information are specifically covered by the requirements of the DPA18 (see Appendix A).

The release or sharing of such data is restricted and all reasonable steps must be taken to ensure that this type of data is safeguarded and not kept for longer than necessary for its purpose.

6.5 **Contemporaneous records** are those that are written at the time.

6.6 **Retrospective records** are those written after the event.

6.7 **Being open and Duty of Candour** is the process by which communication between healthcare staff and a patient (and/or their carers) is open and honest when a patient has suffered harm as a result of healthcare treatment.

6.8 **Records life cycle** describes the life of a record from its creation/receipt through the period of its ‘active’ use, then into a period of ‘inactive’ retention and finally the confidential secure disposal or permanent preservation.

6.9 **A Document** - provides guidance and/or direction for performing work, making decisions, or rendering judgments which affect the quality of the products or services that customers receive. A document should be construed to mean any physical guide or direction whether written, video tape, physical sample, sample drawing, computer program or otherwise.

6.10 **A Record** - proves that some type of required quality system action took place. Sometimes documents become records. For instance, Management Review Minutes become the record that a Management Review has taken place.

- Records are available when needed - from which the organisation is able to form a reconstruction of activities or events that have taken place.
- Records can be accessed - records and the information within them can be located and displayed in a way consistent with its initial use, and that the current version is identified where multiple versions exist.
- Records can be interpreted - the context of the record can be interpreted: who created or added to the record and when, during which business process, and how the record is related to other records.
- Records can be trusted – the record reliably represents the information that was actually used in, or created by, the business process, and its integrity and authenticity can be demonstrated.
- Records can be maintained through time – the qualities of availability, accessibility, interpretation and trustworthiness can be maintained for as long as the record is needed, perhaps permanently, despite changes of format.

- Records are secure - from unauthorised or inadvertent alteration or erasure, that access and disclosure are properly controlled and audit trails will track all use and changes. To ensure that records are held in a robust format which remains readable for as long as records are required.
- Records are retained and disposed of appropriately in compliance with the Records Management Code of Practice 2021 which has been adopted by KMPT for consistent retention and disposal procedures, which include provision for appraisal and the permanent preservation of records with archival value.
- The organisation has an off-site records storage contractor with whom records are securely stored.
- The Information Governance and Records Management Department hold a list of all records stored in off-site storage and they hold a record of authorised users who are permitted to retrieve records from off-site storage. They also maintain a record of all records that have been sent for destruction and the related destruction certificates.
- Staff are trained - so that all staff are made aware of their responsibilities for record-keeping and record management.

6.10 **Information/Records Systems** – can be manual or electronic changes or new systems that process data and therefore create records must be authorised by senior management within KMPT in consultation with Digital Services. They must be checked to ensure they comply with data protection requirements and approved by the Information Governance and Records Management Department, who will undertake a data protection impact assessment (DPIA) in line with the Trusts Privacy by Design and Default Policy.

6.11 **Protective Markings** - Protective marking denotes how a document should be treated, which affects how a document is saved, stored, transferred and whether it may be disclosed.

File markings reflect the level of security measures necessary to protect the information contained within a file or document. It is important that all trust documentation carries the appropriate markings in order to protect privacy and confidentiality. Understanding the status of a file helps readers to make appropriate decisions about distribution and storage.

The overall policy for healthcare on restrictive marking is set by the cabinet office and is called the government security classification scheme (GSCS). It applies across all government, including the NHS and relevant partners. From 2014 onwards, all information below **SECRET** level is to be classified **OFFICIAL**. Individuals are expected to take more personal responsibility for thinking about the security of the information they handle.

Under the NHS code of practice all patient information is to be treated as **CONFIDENTIAL**. All documentation is held to be **OFFICIAL**; consequently, there is no requirement to explicitly mark routine information with the **OFFICIAL** classification.

In addition, the NHS Code of Practice defines descriptors applicable to data produced by, or relevant to, the conduct of NHS business and activity, as follows:

COMMERCIAL, to identify market-sensitive information, including that which is subject to statutory or regulatory obligations that may be damaging to the trust

PERSONAL, to identify personal data defined under the Data Protection Act (2018), the release or loss of which could cause harm, distress or detriment to the individual(s) to whom it relates
LOCSEN, to identify information which is locally sensitive to the trust itself or to a recipient trust or other organisation within the NHS

7 LEGAL AND PROFESSIONAL OBLIGATIONS

The main statuary requirements for records management are as follows:

7.1 **Data Protection Act 2018 (DPA18)**
The Act regulates the processing of personal data. Personal data is defined as – 'data relating to a living individual that enables them to be identified either from that data alone or in conjunction with other information which the data controller i.e. the organisation, holds e.g. name, address, age, race, religion, gender and physical, mental or sexual health'.

The DPA covers all personal information held in both paper and electronic format and applies to all processing of personal information i.e. holding, obtaining, recording, using, disclosing/sharing and secure destruction.

A request for personal information is known as a 'right of access' request, or subject access request and the statutory timescale to comply with such a request is one month from the date of receipt. These requests are processed by the Information Governance and Records Management – Access Team.

7.2 **Freedom of Information Act 2000 (FOIA)**
The Act introduces a greater culture of openness regarding corporate information held by public authorities and covers all information a public authority holds in both paper and electronic format i.e. letters, reports, minutes, emails etc.

The disclosure of personal information i.e. patient and staff records, are exempt under section 40 of the FOIA and must be requested via a subject access request.

All requests for information under FOIA should be in writing. The statutory timescale to comply with such requests is twenty working days. These requests are dealt with centrally by the Information Governance and Records Management – Access Team.

7.3 **Common Law Duty of Confidentiality**
All NHS bodies and those carrying out functions on behalf of the NHS e.g. contractors are under a common law duty of confidentiality regarding personal information. This duty of confidence continues after an employee or contractor has left the NHS.

All Trust staff are advised and informed regarding their duty of confidentiality on commencement of their employment and it is included within the following:

- Job Description
- Employment Contract
- Induction
- Confidentiality Code of Practice
- Annual mandatory Data Security Training for staff.

7.4 Caldicott Principles

The Caldicott principles outline seven areas that all health and social care staff are expected to adhere to in addition to the Data Protection Act. These Principles are:

- Justify the purpose(s) of using confidential information
- Only use it when absolutely necessary
- Use the minimum that is required
- Access should be on a need to know basis
- Everyone must understand their responsibilities
- Understand and comply with the law
- The duty to share information can be as important as the duty to protect patient confidentiality.

7.5 NHS Care Record Guarantee

To maintain the confidence of individuals the NHS and Social Care 'Care Record Guarantee' outlines 12 record keeping guarantees, one of which is that records must be held so that only authorised staff can access them and it will be possible to tell who has accessed the record and when.

8 RECORDS LIFECYLE - CLINICAL AND CORPORATE RECORDS

The Trust has classified the following steps as the lifecycle for KMPT managed records creation, filing, retention, access and disclosure, archiving, closure and transfer, appraisal and destruction.

8.1 Creation

Wherever possible, within our services, patients will have a single, structured, multi-professional and agency record (Rio) which supports professional and integrated care.

All services should have in place a process for documenting its activities in respect of records management. These processes should consider the legislative and regulatory environment in which the Trust operates. All records should be complete and accurate, to facilitate and audit or examination of the organisation, its patients, staff and other affected by its actions, and provide authentication of the records so that evidence derived from them is shown as credible and authoritative.

All records created by the Trust must be arranged in a record keeping system with a unique identifier that enables the quick and easy retrieval of information. Electronic and paper records held in record keeping systems should be named appropriately to enable the system to operate efficiently and effectively.

An effective records management service depends on knowing what records are held, where they are stored, who manages them, in what format(s) they are made accessible and their relationship to trust functions i.e. healthcare, HR, finance etc.

It is good practice to note the date the file was created and the date it is due to be closed and reviewed, archived and/or destroyed.

Poor record keeping can lead to significant and costly consequences, for example by negatively affecting patient care, law cases against the trust, individual staff dismissal, or monetary fines.

8.2 Filing

All records, electronic or paper, created by the Trust must be arranged in a record keeping system that enables the quick and easy retrieval of information. The agreed filing structure should also help with the management of the retention and disposal of records.

A referencing system should be used that meets the organisations business needs, and can be easily understood by staff members that create documents and records. Several types of referencing can be used, for example, alphanumeric; alphabetical; numeric; keyword.

It may be more feasible in some circumstances to give a unique refence to the file or folder in which the record is kept and identify the record by reference to date and format.

8.3 **Retention**

It is a fundamental requirement that all records are retained for a minimum period of time for legal, operational, research and safety reasons. Please refer to the Trust's Retention and Destruction Policy for further details on the retention periods relevant to Trust records as detailed in the NHSX Records Management Code of Practice 2021.

To ensure the legal and statutory requirements are met, with regards to the retention periods of records, the Information Governance and Records Management Department should be notified of any new types pf records that do not appear in the NHSX Records Management Code of Practice 2021, so that a lifecycle for the record is determined at the point of creation.

8.4 **Maintenance**

There should be no creation of new paper records, all records where applicable must be recorded on electronic systems. Where this is not possible for example with clinical records where temporary inpatient ward files are required or paper psychometric test papers are completed the front cover must contain:

- Full Name
- Date of birth
- NHS Number
- Description of contents

If alterations need to be made to any paper records then these can be made by simply scoring out with a single line followed by the correct entry, with date, time and signature and designation, and must be countersigned by a registered member of staff. Correction fluid must not be used.

If any information is found to be inaccurate, misleading or misreported within clinical records then this must be communicated in writing to the Information Governance and Records Management Department for processing under an individual's 'right to rectification'.

Any information or document(s) that are uploaded or marked on a patient record in error and should be reported to the Clinical Systems Team for Trust processes to be followed in order for removals or amendments to be made to the electronic record.

8.5 **Access and Disclosure**

Access to all records must be restricted to authorised personal wherever they are stored and records must be securely locked away. All staff are aware that they are not permitted to access information held by the Trust without a legitimate need even if their security level allows access. All requests for access to or copies of information held by the Trust must be referred to the Information Governance and Records Management – Access Team. This does not prevent staff from sharing information where risk outweighs confidentiality.

8.6 **Archiving**
Weeding/decanting is the process by which records are selected as inactive (not current) and either transferred to a digital archive area on the Trusts secure network or if paper records, to an offsite storage site with the Trusts approved contractor.

All archiving is completed by the Information Governance and Records Management Department, who are also responsible for the retrieval of archived records.

8.7 **Closure and Transfer**
Records should be closed as soon as they cease to have current business value. Closed records should not be altered, and should be used for reference purposes only. Where it is necessary to change a closed record, an audit of the change should be recorded and kept with the original record. Closed paper records should be sent to the Information Governance and Records Management Department to be processed in line with the Trusts Retention and Destruction policy. Closed digital records should be indicated as such on the digital record storage system.
Movement of any records (even on the same site), should always be logged in inventory format. If physically transporting personally identifiable data or confidential records then please refer to the Trusts Information Security Policy.

8.8 **Review**
When business use for a record has ceased, the records must be reviewed. There will be one of three outcomes from the appraisal of a record:

1. destroy/delete
2. retain for a longer period
3. transfer to a place of deposit under the Public Records Act (1958).

Any permanent preservation of records should be undertaken in consultation with the Head of Information Governance and Records Management. If a decision is made to destroy a record there must be evidence of the decision, and justification for doing so (e.g. duplicate record, past retention period).

8.9 **Destruction**
Records must only be destroyed under confidential conditions using an approved contractor, authorised by the Caldicott Guardian and DPO and a certificate of destruction will be stored centrally by the Information Governance and Records Management Department. A register of the records being destroyed should be kept which shows:

- The record reference (a summary of the record)
- Justification for destruction (from the appraisal)
- Date of destruction

9 CLINICAL RECORD KEEPING DUTIES AND RESPONSIBILITIES

9.1 Any staff member, whether clinical, administrative, qualified or unqualified, who is required to make entries into a clinical record as part of their role, has a duty and professional responsibility to ensure that entries are completed in line with the record keeping standards. This applies whether the record is held by the patient, in paper or electronic format.

Kent and Medway NHS and Social Care Partnership Trust (KMPT) uses an electronic record system, Rio, and this is the Trust's primary record.

8.2 Record keeping is essential to patient care and professional practice, and the law places equal value on care and documentation. The quality of the records of care is a direct reflection of the standard of clinical practice. Good record keeping practice is evidence of a skilled and safe practitioner, incomplete records will create a poor representation of practice.

8.3 Clinical records are legal documents and care should be taken by staff in their creation, recording and management. These Standards are to assist in producing high quality and timely patient records.

8.4 Entries in health records must include information on accountability and responsibility for the patients care, assessment details, risk assessments, plans of care, members of staff involved and how, what occurred and when, and follow-up action necessary in order to support effective clinical judgements / decisions and support effective continuity of care.

9.5 As a member of the health care team, the health care staff entering information into a patient's record takes personal accountability for good record keeping. They must keep clear, accurate and timely records of care they provide to their patients to support communication, continuity and decision making. This includes all forms of patient records, such as anything that is documented about a patient and his/her care and treatment.

8.6 Record keeping is an integral part of every intervention and the member of staff should be assessed as competent in the complete provision of care, which includes record keeping.

8.7 Good record keeping can determine accountability, facilitate clinical decision making, improve patient care through clear communication of the treatment rationale progress, provide a consistent approach to team working and help defend complaints or legal proceedings.

8.8 The NHSX Records Management Code of Practice for Health and Social Care 2021 has been published as a guide to the required standards of practice in the management of records for those who work within, or under contract to NHS organisations in England. The Code also applies to adult social care and public health functions commissioned or delivered by local authorities. It is based on current legal requirements and professional best practice, which therefore has informed the development of this policy and subsequent procedures in place across the organisation.

NHSX_Records_Management_CoP_V7.pdf (england.nhs.uk)

10 RECORDS MANAGEMENT STANDARDS – CLINICAL RECORDS

All registered health professionals are accountable for the content and quality of all their entries into the Clinical Record and must adhere to, and meet Kent and Medway NHS and

Social Care Partnership Trusts Record Keeping Standards and their Professional Regulatory Body.

Unregistered health professionals and trainees/students must comply with local guidelines for delegation of responsibility only those listed in Appendix D may write to the electronic patient record in their own name.

All staff are reminded to not attempt to interpret data held within a patient's clinical record if they are not qualified to do so, it is essential that staff seek the help and guidance from qualified colleagues to ensure the correct interpretation.

The principles of documenting in patient health records are the same for both written and electronic records.

10.1 Electronic Clinical Record Keeping Systems

10.1.1 Electronic Health Records in use within KMPT, which include Rio, PADS and ELMS must only be accessed on Trust issued equipment and only by those authorised to do so.

10.1.2 Electronic Health Records may only be accessed in accordance with the Berkshire Healthcare Policy using the Smart card System IT or relevant access system. Staff must have a legitimate reason to access a patient record. If requested the person accessing the record should record the reasons for access to a particular record.

10.1.3 All electronic records must be validated at the time of entry. All entries into Clinical Records must be validated. All staff, including students and unqualified staff must validate their entry at the time of entry. The quality and content of the record will be monitored through managerial supervision.

10.1.4 KMPT recognise that on occasions there will be clinical documentation produced or received into the Trust that should not be uploaded to the patient's primary electronic record. For example –

- MAPPA meeting minutes/MARAC information – a summary of this type of information should be inputted into the electronic patient record, however for storage of these documents please refer to the Multi Agency Public Protection Arrangements (MAPPA) Policy.

10.1.5 All Rio patient records must be synced to the National Spine. If when entering the patient's record an orange banner is presented then steps must be taken to update the required fields to ensure that local and national data match.

10.1.6 Psychological Testing – Raw Data completed test papers must now be uploaded onto the electronic patient record Rio. Test paper will be uploaded with an additional disclaimer to ensure unqualified staff do not attempt to interpret and to ensure that this data is only released following internal Trust policy.

10.2 Paper Clinical Record Keeping

10.2.1 In accordance with the NHSE long term plan, KMPT are committed to using electronic methods as the preferred mode of recording and storage for patient clinical records. However, it is recognised that sometimes this will not be possible, and accepted that the following areas may hold a secondary paper file -

- Ongoing inpatient documentation
- Highly sensitive or restricted access information
- Documents where a clear scanned copy or transcription cannot be completed.

10.2.2 All written records must be legible and written in permanent ink, with the following information clearly displayed on the outside of the folder cover –

- Patient First Name and Surname
- Date of Birth
- NHS Number
- Temporary folder sticker

Only KMPT blue secondary folders must be used.

10.2.3 Secondary folders being used for the temporary storage of ongoing inpatient documentation must be securely stored away from persons who do not have a legitimate reason to access the information contain within, i.e. locked office or cabinet. Disclosure of the content of records to an individual who does not have a legitimate need to access them constitutes a breach of confidentiality.

10.2.4 Once a patient has been discharged, or the records contained within the secondary folder reach one month since creation the folder should be sent within post bags, mail tough or boxes via internal mail clearly labelled to the Information Governance and Records Management Department for uploading to the electronic patient record.

10.3.6 If secondary folders are lost or mislaid, this could result in a permanent loss of records leading to inadequate treatment for a patient. It could also result in non-compliance with the Trust's legal requirements to access to records requests which can lead to disciplinary action, and in worst cases, a legal claim against the Trust and staff members involved. An incident report should be made on Datix/Inphase and immediate contact made with the Information Governance and Records Management – Security Team kmpt.infosecurity@nhs.net detailing what action ahs been taken to locate the folder.

10.2.7 Secondary folders must never be sent outside of the Trust. All requests for continuing care information must be submitted to the Information Governance and Records Management – Access Team kmpt.infoaccess@nhs.net

10.2.8 All staff are reminded that the use of paper diaries for any clinical contact reason is forbidden, this is due to the issues surrounding the security of diaries and high risk of loss of data if not transferred into the primary electronic patient record. All clinical contact must be recorded and outcomed within the Rio diary.

10.2.9 All staff are reminded that they are not permitted to print copies of patient records from Rio, unless absolutely necessary for business continuity reasons and where appropriate security measures are in place to protect the data. Paper records hold a higher level of risk and this responsibility rests personally with the member of staff who has printed the records.

10.2.10 If paper records need to be transferred off site for example, with a patient who is escorted to an acute trust for physical health reasons, they must be kept secure at all times and never be left unattended during transit for any reason e.g. in a car boot.

10.3 Patient Identification

10.3.1 As of September 2009, it was mandated that NHS numbers must be recorded on all active patient records and for all communications in relation to patient care. The NHS number replaces all local identifiers, however can be used in conjunction with local identifiers where necessary.

10.3.2 Patient safety is the key driver for this change, and the correct and consistent usage of the NHS number eliminates duplicate records in clinical systems which can pose a risk to the patient. There are instances whereby patients may have changed their name or provided false information so it is important to also check with an individual if they have ever received treatment within KMPT.

10.3.3 Staff must avoid keeping copies of information in areas outside of the primary clinical record, for example, the storage of clinical letters on a shared drive as well as being held in the primary record. Where information is in the process of being transcribed these may be stored on a service's shared drive however they must be completed and uploaded to the primary record and deleted from the shared drive. Person identifiable information must not be kept/stored within staff personal (H:) drives.

10.3.4 Due to the nature of the care and treatment provided by KMPT there are often temporary inpatient files or archive paper files that relate to a patient.

10.4 Timeliness of Entries

10.4.1 Entries must be recorded as soon as possible but no longer than 24hrs, after the event has occurred. In situations where this is not possible a progress note should be entered onto the patient record retrospectively.

10.4.2 The electronic patient record maintains an audit trail which automatically records access to the record through the use of 'Smartcards' which provides evidence of authorship and designation of practitioner who created the entry. Smartcards and individual logins should only be used by the designated owner of the Smartcard to ensure that entries and alterations can be traced to a named individual at a given date and time, and on subsequent review any decision making can be justified.

10.5.3 Any physical documentation that must be entered onto the electronic patient record or stored securely on the Trust network must be scanned and stored within 72 hours of write up or receipt. The only exception to this is in relation to Drug Charts and Discharge Prescription Sheets (TTOs) which must be scanned and uploaded within 24 hours of discharge or receipt.

10.5 Information Sharing and Informed Consent

10.5.1 All staff must document in the electronic patient record the discussions they have with patients or their representatives relating to consent at the commencement of any intervention, assessment or treatment.

10.5.2 There is a dedicated Information Sharing and Consent Form that must be completed or reviewed at every interaction with the patient, where able, and at a minimum of every six months.

10.6.3 Where it is suspected/known that a patient does not have capacity to give consent to their care or treatment staff should refer to the Mental Capacity Act Code of Practice and Best Interest Decisions for current guidance on how to proceed. Further information relating to sharing information can be found in the Overarching Information Sharing Policy and Sharing Personal Information Policy.

10.6 Quality of Clinical Records

10.6.1 Clinical records must be complete, consistent, accurate and consecutive. It should be clear in the record whether a statement is fact, patient reported, hypothesis or formulation.

10.6.2 The patient record should clearly demonstrate continual assessment of the patient, identification of patient problems/ concerns / issues, management of risk, clinical reasoning for care given and details of the intervention with outcomes as appropriate.

10.6.3 Clinical Records should be factual and without personal opinion or judgement, they must not include unnecessary abbreviations, jargon, meaningless phrases or irrelevant speculation or any coded expressions of sarcasm or humorous abbreviations to describe the patient/client.

10.6.4 All relevant medical observations: examinations, assessments, tests diagnoses, prescriptions, other treatments taken or given by the Clinician should be recorded in the Clinical Record. This should also include information that the Clinician has access to and is relevant to the patient's care.

10.6.5 Other relevant information / forms / assessments such as Assessment of Capacity (Mental Capacity Act), Lasting Power of Attorney, Advanced Directives or Statements should also be contained within the Clinical Record. These should be regularly reviewed in accordance with need and regulations.

10.6.6 There should be evidence of risk assessment of the patient and / or analysis of their presenting problems. The rationale or reasoning behind the subsequent decisions, care plan and interventions should demonstrate in the Clinical Record.

10.6.7 Any changes to patient's status or care are recorded in the health records. The record should identify risks and enable early detection of complications and allow action to be taken. When risk to the patient or others is documented as changing there should be evidence of changes in the risk rating and care plan.

10.6.8 Where care is planned, involvement of the patient in decisions and planning should be documented in the records. Good record keeping involves documenting discussions with the patient and members of the care team. There should be evidence of consent to treatment.

10.6.9 Relevant disclosures by the patient – pertinent to understanding the cause or affecting the care/treatment of the illness should also be documented. In case where there is an existing and current risk to others (safeguarding) this information may be required to be shared without consent of the patient.

10.6.10 Details of facts and information given to the patient: this should include details of relevant conversations with the patient (including their understanding) and information about their condition, exercises, drugs and medication and includes printed information both internal and external to Berkshire Healthcare.

10.6.11 Designation and recording of information about other people involved in the patient record. When recording contact with other professionals, the full name and designation of the professional should be documented

10.6.12 Alerts, allergies, drug reactions, details of medical implants or similar information must be documented in the relevant place on the Clinical Record, depending on whether it is paper or electronic.

10.6.13 Correspondence and communication to and from the patient and / or other parties should detail the context of correspondence / communication and the persons involved. It should also document any action or inaction resulting from it.

10.6.14 Emails must not be scanned or copied and pasted directly into the progress notes however a summary of the email conversations should be entered. If a whole email conversation is relevant then this may be uploaded into the document secti

10.6.15 on of the records with a corresponding summary within the progress notes.

10.7 Abbreviations

10.7.1 Where it is identified that abbreviations are a practical necessity which will enhance the quality of record keeping, they should be recorded in full on the first occasions with the abbreviation in brackets and there after the abbreviation can be used. If there is any doubt or risk of misunderstanding, it should be written in full.

https://www.kmpt.nhs.uk/information-and-advice/kmpt-acronym-buster/

https://www.nhs.uk/nhs-app/nhs-app-help-and-support/health-records-in-the nhs-app/abbreviations-commonly-found-in-medical-records/

10.8 Clinical Documentation

10.8.1 It is recognised that different services and specialities require specific documentation to meet their professional requirements. However, KMPT is keen to ensure a consistency in the documentation used across the whole organisation. Any documentation used within patient records must be approved by the Information Governance and Records Management Department, who will work closely with the Communications Team to ensure that the Trust's standard layout and formatting is used.

10.8.2 KMPT is also keen to uphold the NHSE requirement to move to a paperless way of working so before any approval of a new paper-based document is provided will refer any request to the Digital Transformation Team for review and response.

10.9 Digital Media Records

10.9.1 It is recognised that the use of electronic devices such as dictaphones, digital cameras and mobile devices is a requirement in some services / departments within the Organisation. As these devices/methods (and their output/media) may not be suitable for encryption, it is important that users consider the confidentiality and security of the information and reduce the risk of loss of any Personal Identifiable Data (PID).

10.9.2 Only Trust issued devices can be used to process patient related data and should be requested directly via the Digital Services Helpdesk 01795508500.

10.9.3 Digital media that needs to be retained specific to a patient should be labelled as with any other record and where practical included in the patient's clinical record. A note of the existence of this digital media record should be made in the clinical notes. If the digital media cannot be stored with the clinical record a note of the storage location must be recorded in the notes.

10.9.4 The digital media should be treated as a clinical record and kept in accordance with relevant policies and guidelines including information security and records retention.

10.10 Scanned Records

10.10.1 When records are scanned in order to be stored electronically it is important that there are processes in place to check the quality and accuracy of the scanning process and the quality and integrity of the final scanned record. Random quality checks comparing scanned and original records should be carried out and documented before the original records are destroyed. Appropriate backup systems must be in place for any systems that include scanned records.

10.10.2 Original records should not be disposed of until the quality check and backup have taken place.

10.11.3 For further information please refer to the Document Scanning Policy and Procedure.

10.11 Complaints

Correspondence that is a result of a complaint, claim or serious incident concerning patients or staff must not be recorded in a patient's clinical records.

10.12 Restricting Access

Access to both paper-based and electronic records should be restricted to service/organisational level. If it is deemed that the record requires further restricting to only a selected group of staff this must be requested via the Information Governance and Records Management Department who will follow the internal processes which ensure consideration is given to the clinical safety of restricting a record.

10.13 Notification of Death

10.13.1 When notification of a death is received, staff must log a call with the Rio System Helpdesk to ensure the records will be updated accordingly. When the death is registered on Rio this will close all open referrals, cancel all appointments, end all Inpatient episodes and close all care plans and assessments. If any paper records are held relating to a patient who has been notified as deceased then these must be returned to the Information Governance and Records Management Department who will review and process the records in accordance with the Trusts retention and disposal requirements.

10.13.2 Records must not be added to following the death of a patient, under the Coroner's and Justice Act 2009 it could be a criminal office of -

- Distorting or otherwise altering any evidence, document or other thing produced or provide for the purposes of a Coroner's investigation;
- Preventing any evidence, document or other thing from being given, produced or provided;
- Intentionally suppressing or concealing a document that the person knows or believes to be a relevant document or to intentionally alter or destroy such a document

10.13.3 If it is identified that an entry should have been made, or document uploaded prior to the patient's death the decision on whether the information should be added must be discussed with the Information Governance and Records Management Department.

10.13.4 If it is deemed that an entry can be made the entry must be headed "Retrospective Entry" and the progress note should record "Retrospective Entry made on dd.mm.yy". The progress note should record what changes, if any, were made into the Rio system e.g. appointment is "outcome" to accurately reflect events and why the entry was made after the patient's death.

10.13.5 If it is deemed that a document can be uploaded to the patients record a note should be added to the description field at the point of uploading stating why the document was uploaded after the death of the patient.

10.14 Transgender Records

10.14.1 NHS England guidance confirms that patients may request to change name and/or gender on their patient record at any time and do not need to have undergone any for of gender reassignment treatment in order to do so.

10.14.2 When a patient changes their name and/or gender, they must notify their GP who will complete the dedicated form available here Adoption and gender re-assignment processes - Primary Care Support England. After this they will be given a new NHS number and will be registered as a new patient at their practice.

10.14.3 At this point a new Rio record will need to be created with the patient's new name and gender and synced to the National Spine which will pull down the new NHS number that has been assigned to the patient.

10.14.4 The old and new records cannot just be merged automatically, likewise the old record cannot be simply deleted. There must be a discussion between the patient and their current treating team to advise that in order to maintain a full history of the care and treatment they have received information from their old record will need to be retained. The following actions must take place –

- Provide the patient with a copy of their old medical records. This can be obtained by contacting the Information Governance and Records Management Department who will follow the Subject Access Request process.
- The patient will then need to meet with the HCP and discuss the content of their old medical record and what the HCP feels should be included in the new record. This should be agreed by the patient, if the patient does not agree, they need to be advised of the risks of this and a note recorded in the old record; the information cannot be transferred into the new record.
- The HCP may want to consider writing a medical record summary to include in the new record; again, the content should be agreed with the patient.
- If redactions are agreed these must be highlighted on a copy of the old medical records and then provided to the Information Governance and Records Management Department who will upload to the new Rio patient record. This should include detail of the old NHS Number.
- If the patient is happy for their old medical records to be simply merged without redactions to their new Rio record then this is their choice. In this instance the HCP should notify the Information Governance and Records Management Department in writing who will log a call for the Rio Systems Helpdesk to merge the old and new record.

10.15 Logically Deleting Rio Records

10.14.5 When a patient applies for a new NHS Number, their old NHS Number is considered to be logically deleted, this in effect means no longer applicable or accessible.

10.14.6 On a weekly basis the Rio Systems Team will receive a report of ‘logically deleted’ NHS Numbers and will perform an exercise to remove these patients’ records from the electronic patient system Rio.

10.14.7 If the patient has an open referral to a service, the Clinical Systems Team will identify the patients new NHS Number and notify an identified HCP within the service the patient is being seen by, of the following;

- The fact the patients old record has been ‘logically deleted’
- The patient new NHS Number
- Dates of planned appointments, so these can be booked again under the new NHS Number
- Request the HCP review a full copy of the old record and copy over, in liaison with the patient where relevant, any clinically pertinent information into the new record.
- The HCP should be provided with temporary access to the ‘logically deleted’ record, so that they can transfer any clinically pertinent information into the new record, noting that this process differs slightly if the logical deletion relates to Section 11.
- If the logical deletion is with reference to a patient changing their name and/or gender then please refer to 10.14.

11 RECORDS MANAGEMENT STANDARDS - CORPORATE RECORDS

11.1 What is a Corporate Record

Corporate records are created in order to ensure that the Trust has the necessary information to deliver high quality services and provide evidence of their activities. Such records must be created and managed to a consistent standard across all services and departments and all staff must adhere to the following principles:

- Individual members of staff are responsible for the information they create.
- All information created by staff as part of their job role contributes to the organisational memory and is evidence of the Trust’s work, and may be needed for reference by others in the future.
- All information is subject to a retention period, specifying how long it must be kept.

11.2 Corporate records can take many forms electronic or paper documents, emails, voice recordings, video recordings and all staff must ensure that the records they create are factual and without personal opinion or judgement, they must not include unnecessary abbreviations, jargon, meaningless phrases or irrelevant speculation or any coded expressions of sarcasm or humorous abbreviations to describe the event, patient/client, colleague etc.

11.3 The Freedom of Information Act 2000 gives a right of access for the public to corporate information held by the Trust. It is therefore necessary that the Trust has systems and processes in place to manage corporate information so that it can be searched and retrieved in order to answer requests for information under the Act.

11.4 Corporate Standards for Ownership of Documents

All records that are produced must adhere to the corporate standards for the records and must contain the Kent and Medway NHS and Social Care Trust logo. The document should specify:

- Author of the document
- The designation of the author e.g. Executive Director of Finance
- The version number of the document
- The date the document was produced

11.5 Naming Convention for Corporate Records

11.5.1 When naming folders, the name should be concise and specific to the contents. Folders that are name after individuals must be SURNAME First name and if relevant a unique identifier for example if the folder is an electronic staff file it should note the employee number e.g. BLOGGS Joe 12345698.

11.5.2 When naming documents/files give it a unique and meaningful name that reflects the contents. All documents and files should be named using a date reference, a description, a version number, author and if in preparation labelled DRAFT.
e.g. 20230224 Overarching Records Management Policy v0.1 AP DRAFT

11.5.3 When naming emails use the same guidance as provided in 11.5.2.

11.6 Storage of Corporate Records – Electronic

11.6.1 Trust records must not be stored on your individual H drive (H:\) as they must be accessible to everyone who needs them. Your H drive is your personal folder provided to you by KMPT on the Trust network and designed to hold information that is relevant to only you.

11.6.2 Trust records must be stored on the S Drive (S:\) which is designed to allow departments and services to share information and work with each other. It is important to understand who else has access to a shared drive, access can only be granted by the Digital Services Team with the folder owners' approval. This is to ensure that all staff are able to make informed decisions about storing records appropriately.

11.7 Storage of Corporate Records – Paper

11.7.1 Paper corporate records should be stored with their creator, or centrally within the department. They must be stored securely, e.g. in lockable cabinets or storage areas to prevent unauthorised access. They must be protected from damage, fire and flood. Its also prudent to remember that records must remain accessible during periods of staff absence.

11.6.2 If a record exists in an electronic format, consider whether keeping a paper copy of the document/file is necessary, for further information please refer to the Retention and Destruction Policy, or contact the Information Governance and Records Management Department 01795514525. Do not keep duplicates of records unless there is a legal reason to do so.

11.6.3 The Information Governance and Records Management Department is committed to working towards the NHSE long term plan ensuring a paper free working environment, which includes the reduction of paper files being stored on Trust site and within off site archives. This includes the digitisation of all staff files with leavers records being held in one central electronic library. If any service holds paper files and requires assistance to scan and hold these electronically they can contact the Information Governance and Records Management Department directly 01795514525.

Personnel Files

11.7.2 Personnel files must comply with the requirements of the Data Protection Act 2018. Employees have a right to see their personnel file held irrespective of whether this is a paper file or held electronically. It is important that managers ensure that only relevant information is held within these files and that they are kept accurate and up to date.

11.7.3 There should only ever be one personnel file for an employee, where an existing member of staff transfer to another job role within the Trust the staff file should be transferred to their new line manager, this must be completed within one week of the member of staff transferring.

11.8.3 For any new employees, employed by the Trust after the 31st March 2023, an electronic personnel file should be created on the Trust secure network within the S Drive. Line managers should contact the Digital Services Helpdesk in order to create appropriate folders.

11.7.4 All staff files must be stored within a secure location i.e. lockable cabinet or on the Trust secure network within the S Drive where access is restricted to the manager or the person designated to maintain the files.

11.7.5 The Information Governance and Records Management Department are committed to assisting all managers across the Trust to transfer paper personnel files to a secure location within the S Drive, if you would like help to complete this for your files then please contact the Department directly on 01795514525.

11.7.6 All managers are expected to ensure that the following information is stored accurately within each personnel file. If a paper file is held then each of the below should be split into sections, and if an electronic file is held then this should be the naming convention of the folders –

- **Absence Management**
  including return to work forms, occupational health reports and FIT notes/ Self Certifications
- **Annual Leave**
  all request and annual leave responses should be recorded on ERoster / Employee Online – training records, appraisals and supervisions should be recorded on iLearn
- **Change Forms**
- **Disciplinary/Grievance**
  initial complaint/grievance/investigation and outcome document should be kept on personnel file and the remaining file must be sent to archive once case and any appeal are closed, or any sanction is spent).
- **Employment Documents**
  contract of employment, job description, references, application form, proof of right to work, proof of ID, proof of professional registration, change forms, maternity/new parent leave documents
- **Health and Safety**
  including DSE's and any other relevant risk assessments
- **HR Documents**
  including capability, probation, flexible working and appeals
- **Paper Record**

for staff who had a paper record and now have an electronic record

- **Training**
  For recording internal and external training

11.7.7 Once a staff member leaves Trust employment the line manager must transfer the personnel file to the information Governance and Records Management Department for archiving and retention in line with the Retention and Destruction Policy.

- Paper Files should be sent via internal mail using the internal post label in Appendix E.
- Electronic Files will need to be transferred to S:\IG_Shared, in order to do this please contact the Information Governance and Records Management – Security Team on 01795514562 who will arrange access to the dedicated folder.

11.7.8 Medical staff files are managed by Medical Staffing, the guidance provided in 11.8.5 and 11.8.6 should be followed when managing these files.

12 EQUALITY IMPACT ASSESSMENT SUMMARY

12.1 The Equality Act 2010 places a statutory duty on public bodies to have due regard in the exercise of their functions. The duty also requires public bodies to consider how the decisions they make, and the services they deliver, affect people who share equality protected characteristics and those who do not. In KMPT the culture of Equality Impact Assessment will be pursued in order to provide assurance that the Trust has carefully considered any potential negative outcomes that can occur before implementation. The Trust will monitor the implementation of the various functions/policies and refresh them in a timely manner in order to incorporate any positive changes.

13 HUMAN RIGHTS

13.1 The Human Rights Act 1998 sets out fundamental provisions with respect to the protection of individual human rights. These include maintaining dignity, ensuring confidentiality and protecting individuals from abuse of various kinds. Employees and volunteers of the Trust must ensure that the trust does not breach the human rights of any individual the trust comes into contact with.

14 TRAINING

14.1 All Trust staff will be made aware of their responsibilities for record keeping and records management through generic and specific training programmes and guidance.

14.2 All clinical staff must as part of their corporate induction complete the e-learning modules on Clinical Record Keeping, Scanning and Uploading Documents to Rio and Data Security and Awareness Training.

14.3 Th Information Governance and Records Management Department are available to provide advice, more specific training and guidance in all areas of clinical and corporate records management.

14.4 Trust staff not registered by a regulatory body must also complete the assessment of competency in record keeping in Appendix C.

15 MONITORING COMPLIANCE WITH AND EFFECTIVENESS OF THIS DOCUMENT

What will be monitored	***How will it be monitored***	***Who will monitor***	***Frequency***	***Evidence to demonstrate monitoring***	***Action to be taken in event of non-compliance***
Quality of Records	Records Auditing	Clinical managers/Care Group Leads & HR	Monthly	Individual supervisions	Local action plans to be implemented – consideration of raising risk on Datix/InPhase.
Quality of Records	Annual Clinical Record Keeping Audit	IG & RM & HR	Annual	Completion of audit forms	Report to IGG and TWPSG Local action plans – consideration of raising risk on Datix/InPhase
Compliance with policy and NHS long term plan	Program of active retention and destruction trust wide	IG & RM and HR	On going	Completion of retention and destruction requirements	Report to IGG. Consider raising a risk on Datix/InPhase

16 EXCEPTIONS

16.1 There are no exceptions to this policy.

APPENDIX A DPA18/UKGDPR PRINCIPLES

(Does not apply after death. Applies to manual as well as electronic records)

When processing personal data, it must be –

1. processed lawfully fairly and in a transparent manner in relation to individuals (‘lawfulness, fairness and transparency’);

2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes (‘purpose limitation’);

3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);

4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data is accurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’);

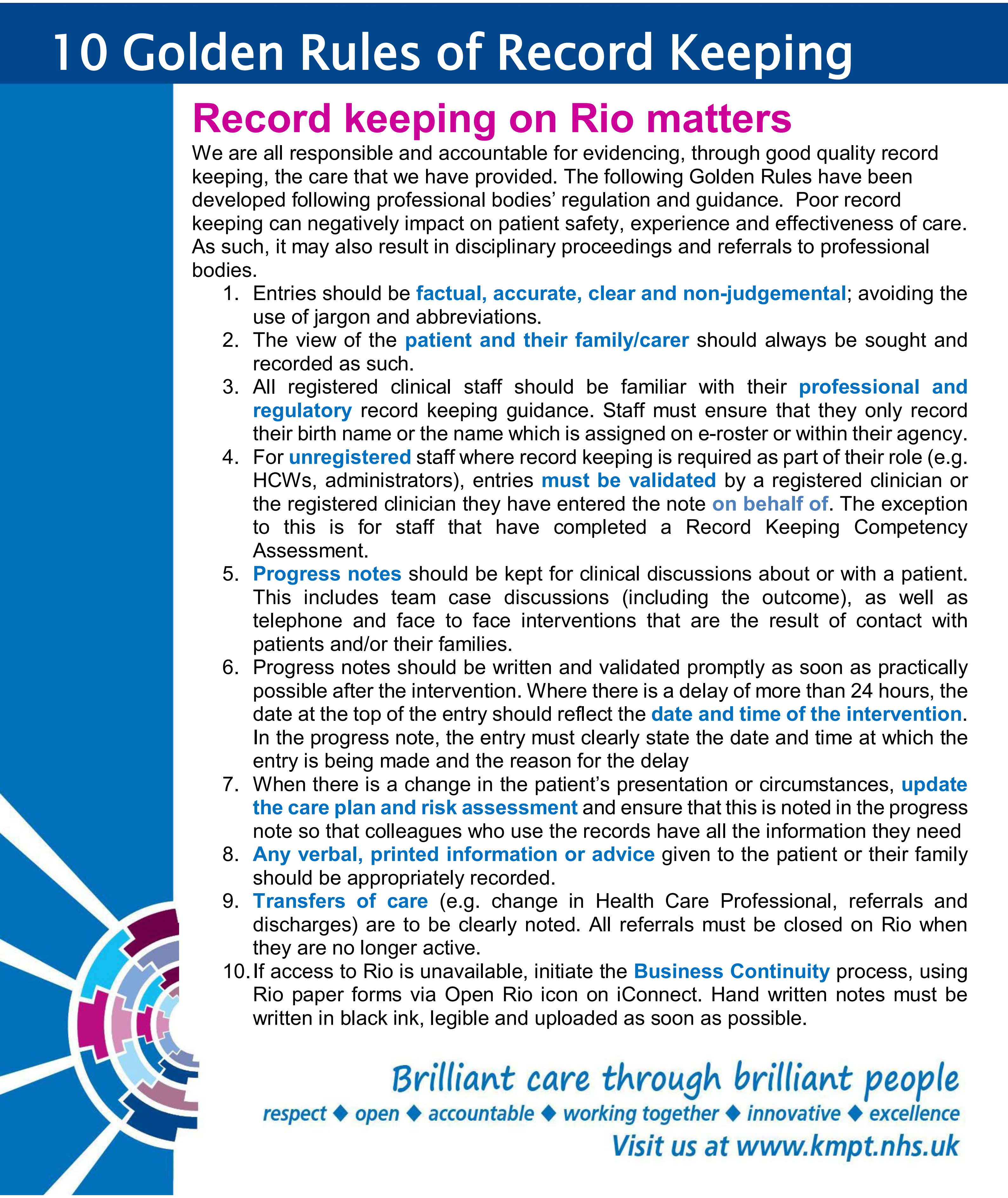
5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are process; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by DPA18/GDPR in order to safeguard the rights and freedoms of individuals (‘storage limitation’);

6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures 9’integrity and confidentiality’)

CALDICOTT PRINCIPLES

1. Justify the purpose.
2. Do not use person-identifiable information unless it is absolutely necessary.
3. Use the minimum necessary person-identifiable information.
4. Access to person-identifiable information should be on a strict need to know basis.
5. Everyone with access to person-identifiable information should be aware of their responsibilities.
6. Understand and comply with the law.
7. The duty to share information can be as important as the duty to protect confidentiality.

APPENDIX B 10 GOLDEN RULES OF RECORD KEEPING



10 Golden Rules of Record Keeping

Record keeping on Rio matters

We are all responsible and accountable for evidencing, through good quality record keeping, the care that we have provided. The following Golden Rules have been developed following professional bodies' regulation and guidance. Poor record keeping can negatively impact on patient safety, experience and effectiveness of care. As such, it may also result in disciplinary proceedings and referrals to professional bodies.

1. Entries should be **factual, accurate, clear and non-judgemental**; avoiding the use of jargon and abbreviations.
2. The view of the **patient and their family/carer** should always be sought and recorded as such.
3. All registered clinical staff should be familiar with their **professional and regulatory** record keeping guidance. Staff must ensure that they only record their birth name or the name which is assigned on e-roster or within their agency.
4. For **unregistered** staff where record keeping is required as part of their role (e.g. HCWs, administrators), entries **must be validated** by a registered clinician or the registered clinician they have entered the note **on behalf of**. The exception to this is for staff that have completed a Record Keeping Competency Assessment.
5. **Progress notes** should be kept for clinical discussions about or with a patient. This includes team case discussions (including the outcome), as well as telephone and face to face interventions that are the result of contact with patients and/or their families.
6. Progress notes should be written and validated promptly as soon as practically possible after the intervention. Where there is a delay of more than 24 hours, the date at the top of the entry should reflect the **date and time of the intervention**. In the progress note, the entry must clearly state the date and time at which the entry is being made and the reason for the delay
7. When there is a change in the patient's presentation or circumstances, **update the care plan and risk assessment** and ensure that this is noted in the progress note so that colleagues who use the records have all the information they need
8. **Any verbal, printed information or advice** given to the patient or their family should be appropriately recorded.
9. **Transfers of care** (e.g. change in Health Care Professional, referrals and discharges) are to be clearly noted. All referrals must be closed on Rio when they are no longer active.
10. If access to Rio is unavailable, initiate the **Business Continuity** process, using Rio paper forms via Open Rio icon on iConnect. Hand written notes must be written in black ink, legible and uploaded as soon as possible.

Brilliant care through brilliant people

respect ◆ open ◆ accountable ◆ working together ◆ innovative ◆ excellence

Visit us at www.kmpt.nhs.uk

APPENDIX C RECORD KEEPING COMPETENCY ASSESSMENT FORM

COMPETENCY CHECKLIST

Full Name (As displayed on Rio/Legal name)	
Team name (As displayed on Rio)	
Full Team Address	
Date	
Assessor Full Name	
Team Name	

This assessment is to be used by all qualified clinical staff when supervising any unqualified clinical staff in order to assess their record keeping competencies with a view to ensuring that they are able to sign them off as being competent to validate their own notes in future. Until a member of staff who is not registered or licensed by a regulatory body has been assessed as competent to make entries into a patient/ client's clinical record independently, they must have all entries countersigned by their supervisor both electronically and in the physical record.

It is recognized that existing custom and practice exists for some unqualified clinical staff for example support workers working in the community, whereby they are not required to have entries countersigned. To ensure a robust all-inclusive governance process those staff are required to undertake the assessment process to continue to practice unsupervised. The list below, although not exhaustive is a guide to those unqualified staff who fulfil this category –

Permanent Healthcare Assistance
Trainee Nursing Associate
Peer Support Worker
Trainee Clinical Psychologists
Nursery Nurse
Occupational Therapy Assistant
Assistant Psychologist
Physiotherapist
Trainee Clinical Associate Psychologists
UMHH Call Handler

Prior to undertaking the assessment process all staff are required to have fulfilled the following:

- Demonstrated a satisfactory level of competence through being supervised and entries countersigned evidenced through the Knowledge and skills Framework and supervision.

- Be up to date with Record Keeping Training.

- Be able to demonstrate a knowledge and understanding of the record keeping policy and the information governance policy.

The Assessment is to be carried out by the member of staff's line manager or an appropriately qualified clinician nominated by them. In most instances this competency assessment will be completed on a once only basis. The assessment process will need to be repeated if the following applies:

- The staff member fails the initial competency assessment and is required to be reassessed
- The staff member has been asked to desist from making unsupervised clinical entries because of poor practice and is required to be reassessed.
- The staff member is not up to date with record keeping training.

Individual staff members practice standards relating to all aspects of record keeping and clinical entries are to be monitored through the audit and supervision process. Where there are minor concerns about quality of practice these are to be addressed within the supervision process. Where there are moderate/major concerns the staff member will be required to undertake the assessment process before continuing to make unsupervised clinical entries.

If a staff member's required level of supervision changes the Rio support team must be informed on the following contact details so the staff member's access rights can be adjusted accordingly - kmpt.riohelpdesk@nhs.net

The completed and signed form must be scanned and emailed to the KMPT system helpdesk email address kmpt.riohelpdesk@nhs.net from the signing managers email address before it can be actioned.

	Competency	**Assessors Signature**	**Staff Signature**	**Date**
Standards relating to written or typed entries				
1	Handwriting is legible and written in black ink to ensure that the notes will be legible in the event that they need to be scanned.			
2	All entries to records are signed and the person's name and job title is printed along with the signature alongside the first entry.			
3	All entries are dated and time entered against them for all records. This is in chronological order and to be made as close to the actual time as possible			
Standards relating to all data entry to Rio				
4	The ward / team name and base/site of person entering the data is clearly indicated in the information entered			
Standards relating to all entries				
5	The entries are accurate, factual, Jargon free, devoid of meaningless phrases or speculation			
6	No unnecessary abbreviations are to be used, including those used to describe service users or any aspects of their care.			
7	Record details of any assessments and reviews undertaken, and provide clear evidence of the arrangements have made for future and ongoing care. This includes: Details of information given about care and treatment. Plans relating to action or treatment must be clearly stated within the records.			
8	At all times Consider and be aware of the limits of role and responsibilities relating to all aspects of record keeping			

9	Entries identify any risks or problems that have arisen and show the action taken to deal with them e.g. handing over to qualified staff.			
10	Communicates appropriately and effectively with colleagues, verbally and through written records ensuring that they have all the information they need about the people in your care.			
User Involvement				
11	The member of staff is able to demonstrate that they have involved the service user/carer in the record keeping process by evidencing the following points in their notes: Confidentiality (and when risk overrides confidentiality). Who they will share information with Consent to the referral Consent to type of information that will be kept on records.			
12	Understand the importance of engaging the service user and carers and evidencing their active contribution to the following aspects of their care: Care planning CPA documentation Advanced directives Mental Health Act Ward rounds/reviews			
13	Write in a way that is easily understood by the service users in your care.			
Storage alteration and disposal of records				
14	The member of staff demonstrates awareness that they must on no account destroy any records without being authorized to do so.			
15	Understand the procedure for altering and saving records within Rio			
16	Demonstrates understanding that Where a clinical record needs to be altered the following is to be carried out: • The original record is to be signed and dated • Confirm that both the alterations you make, and the original record, are clear and auditable.			
17	Demonstrates understanding that Under no circumstances are records to be falsified			
Legislation, Policy and Guidance				
18	Is aware of and has knowledge of Caldicott Guidance			
19	Is aware of and has knowledge of Data Protection Act and information Governance Policy.			
20	Is aware of and has knowledge of Clinical Records Policy			
21	Is aware of and has knowledge of their profession's record keeping standards.			
22	Has attended Record Keeping training			
23	Has attended Rio Training			

I have conducted the above assessment and the staff member is:

Competent   Not Competent

Signed   (Assessor)……………………………

Designation…………………   Date……………...

Signed (Staff member) …………………………

Designation…………………   Date……………...

(Please make any relevant notes below)

On completion of this form it should be forwarded to the Manager/Modern Matron for filing within the person's individual personal file and a copy given to the staff member for their continuing professional development folder and a copy sent to the KMPT system support team on the email address below

Email address for System Support Team

kmpt.riohelpdesk@nhs.net

APPENDIX D CLINICAL RECORD VALIDATION GUIDANCE

This guidance outlines the standards for the entry and validation of clinical information and the responsibilities of staff and their managers.

All progress notes **MUST** be validated.

A progress note must be validated once completed; On occasions where there is a requirement to validating the work of others this is not to confirm you witnessed the activity but that the content of the note is inoffensive and factually correct (i.e. not conjecture). The following issues will arise if notes are not validated:

- Notes will not pull through to the significant events timeline (this is where staff are able to view events marked or set as significant in a chronological order).
- Notes tagged as a risk event, if un-validated will not pull through to the risk overview.
- Notes can be edited by anyone; they remain in draft. If another user clicks into a draft note, the note detail will show that it was last edited or updated by that staff member even if they did not change anything. If anything is changed a history of changes to drafts is not kept therefore it is not possible to review what was altered or deleted.

Progress note entries are a vital source of clinical information and it is imperative that the recording of clinical information is **Accurate, Relevant, Complete and Contemporaneous (i.e. timely, up to date).**[1]

In-patient/CRHT progress notes must be entered the same day i.e. before the end of the shift. Staff should not, wherever possible leave a shift without validating their work. Students or non-registered staff have a responsibility to seek out their colleagues or mentors to ensure notes are signed before they leave shift. If there is a reason a note was not validated it must be validated ASAP.

Community progress notes should be entered immediately after the interaction or as soon afterwards as possible. It is the responsibility of non-registered or student staff to seek out their colleagues or mentors to have notes signed off before completing their working day. If there is a reason a note was not validated it must be validated ASAP.
The date of the note must always be the date and time the event occurred for it to appear chronologically within the notes. The Rio system date stamps the note so an audit of when it was actually entered into the system is available (click note detail).

Staff without validation rights

- Some students/trainees will not have validation rights (please see Appendix C for list)
- Admin staff will not have validation rights.
- Healthcare Assistants (unless they have completed the competences (see appendix 1). will not have validation rights.

Admin Staff are only permitted to write into progress notes on behalf of a registered healthcare professional. The content of the progress note must then be checked by the registered healthcare professional and then validated.

Prior to validating a progress note, the content must be checked to ensure that it meets the standards as set out in Appendix F. The member of staff is accountable for the standard of the note they are validating ensuring it meets the “10 Golden Rules for Record Keeping”.

Staff with validation rights -

- Registered staff
- Untrained clinical staff that have completed the competencies (see appendix C).
- Where a line manager disagrees with a validated entry they must make an additional separate entry stating this. This entry must be dated and timed to immediately follow the one they disagree with.
- Staff with validation rights are validating to confirm that a suitable note has been entered.

Supervision

- Un-validated notes should be reviewed and discussed as part of staff management and supervision. BI reports are available from the Information Team to support the checking of un-validated notes. There are also reports within Rio itself which show unvalidated notes by user and team. This can be found in the User View.

Competencies

- Non-registered staff can complete a Record Keeping Competency Assessment (Appendix C). Following successful completion staff are assessed as competent to validate their own notes.

APPENDIX E ADDRESS LABEL & CONTENTS LIST

PRIVATE & CONFIDENTIAL

INTERNAL POST

INFORMATION GOVERNANCE & RECORDS MANAGEMENT DEPARTMENT
1st Floor
Magnitude House
New Hythe Lane
Aylesford
Kent
ME20 6WT

RETURNED RECORDS - CONTENTS LIST	
Team/Department	
Name and Contact Details of Sender	
Type of Records	
Further Details:	

APPENDIX F MANAGERS GUIDANCE FOR PERSONNEL FILES

Kent and Medway
NHS and Social Care Partnership Trust

MANAGERS GUIDANCE FOR PERSONNEL FILES

How personnel files must be held

All **new employees** employed by the Trust from **March 2023** must have an **electronically held personnel file.** Line managers should contact the Digital Services Helpdesk on, 01795508200, in order to create appropriate folders.

1. All staff files must be stored within a **secure location.** Where a **paper personnel file** exists (for staff employed prior to March 2023) these should be kept in a **secure location** i.e. lockable cabinet. For electronic personnel files these should be kept on the Trust secure network within the S Drive where access is restricted to the manager or the person designated to maintain the files.
2. The Information Governance and Records Management Department are committed to assisting all managers across the Trust to **transfer paper personnel files to a secure location within the S Drive**, if you would like help to complete this please contact the Department directly on 01795514525.
3. There should only ever be **one personnel file** for an employee, where an existing member of staff transfer to another job role within the Trust the staff file should be transferred to their new line manager, this must be completed within **one week** of the member of staff transferring. Request for transfer of electronic personnel files should be raised by the manager with current access to the personnel file via the Digital Services Helpdesk, providing details of the new manager for the file to be transferred to.
4. All managers are expected to ensure that the following information is **stored accurately** within each personnel file. If a **paper file** is held then each of the below should be **split into sections**, and if an **electronic file** is held then this should be the naming convention of the **folders** –
   - ✓ **Absence Management** - including return to work forms, occupational health reports and FIT notes/ Self Certifications
   - ✓ **Annual Leave** - all request and annual leave responses should be recorded on ERoster / Employee Online – training records, appraisals and supervisions should be recorded on iLearn
   - ✓ **Change Forms**
   - ✓ **Disciplinary/Grievance** - initial complaint/grievance/investigation and outcome document should be kept on personnel file and the remaining file must be sent to archive once case and any appeal are closed, or any sanction is spent).
   - ✓ **Employment Documents** - contract of employment, job description, references, application form, proof of right to work, proof of ID, proof of professional registration, change forms, maternity/new parent leave documents
   - ✓ **Health and Safety** (including DSE's and any other relevant risk assessments)
   - ✓ **HR Documents** - including capability, probation, flexible working and appeals
   - ✓ **Paper Record** - (for staff who had a paper record and now have an electronic record)
   - ✓ **Training** - For recording internal and external training
5. Once a staff member leaves Trust employment the line manager must transfer the personnel file to the information Governance and Records Management Department for archiving and retention in line with the Retention and Destruction Policy.
   - **Paper Files** should be sent via internal mail to the Information Governance and Records Management Department, St Michaels House, St Michaels Road, Sittingbourne, ME10 3DW.
   - **Electronic Files** will need to be transferred to S:\IG_Shared, in order to do this please contact the Information Governance and Records Management – Security Team on 01795514562 who will arrange access to the dedicated folder.

Brilliant care through brilliant people

respect ◆ open ◆ accountable ◆ working together ◆ innovative ◆ excellence

Visit us at www.kmpt.nhs.uk