NHS
Bridgewater
Community Healthcare
NHS Foundation Trust

Records Management – Storing and Movement of Records Policy

Policy Number	**IG/Pol/013**
Target Audience	**All Bridgewater staff including agency, locum, bank workers and learners in practice**
Lead Executive Director	**Chief nurse/deputy CEO**
Recommending Committee/Group	**DIGIT**
Approving Committee	**Corporate Clinical Policy Group**
Ratifying Committee	**Corporate Clinical Policy Group**
Date First Ratified	**November 2018**
Last Full Review Date	**March 2024**
Next Full Review Date	**March 2026**
Extension agreed to	**N/a**
Policy Author	**Information Governance and Records Manager**
Version Number	**3**

Applicable Statutory, Legal or National Best Practice Requirements	Data Protection Act 2018, c.12 National Data Guardian (2024) National Data Guardian 2022-2023 report Freedom of Information Act 2000 NHS Digital. Data Security and Protection Toolkit assessment guides 2023-2024 (version 6 standard) NHS Digital (2021) Data Security and Protection Toolkit NHS England (2014) National health visiting service specification 2014/15 NHSx (2021) Records management code of practice for health and social care NHS England (2022) High quality patient records Public Health England (2015) Child health information systems Public Health England (2015) Output and information requirements specification

Document classification: OFFICIAL-SENSITIVE: Commercial
Document retention – lifetime of the Trust or 20 year review
Document owner – Information Governance and Records Manager

The Trust is committed to an environment that promotes equality, embraces diversity, and respects human rights both within our workforce and in service delivery. This document should be implemented with due regard to this commitment.

This document can only be considered valid when viewed via the Trust's intranet. If this document is printed into hard copy or saved to another location, you must check that the version number on your copy matches that of the one online.

Version Control Sheet

Version	Date	Reviewed By	Comment
1.0	1/8/18	S. Ramsdale	First Draft
	14/11/18	Policy Approval Group	Approved following minor typo changes
	Nov 2018	S. Ramsdale	Amendments completed
	Nov2018	S. Arkwright	Approved by chair action
2.0	December 2019	S Ramsdale	Updated section 7.1 children's records, clarification on movements of records as per
	January 2020	J. McKay	Task and finish group on transfer of children's records Minor amendments following comments from S. Arkwright
	January 2020	S. Arkwright	Approved by chair action
	December 2021	J McKay	Review
	December 21	DIGIT	Signed-off
	Dec 2021	M. Corkery	Comments made
	January 2022	Corporate Clinical Policy Group	Approved subject to amendment to S. 4
	January 2022	J. McKay	Amendments completed
	January 2022	J. Hogan	Approved by chair action, submitted to Trust Board for ratification
	3rd February 2022	Trust Board (e-governance)	Ratified – Policy Officer notified 28/02/2022
2.1	January 24	J. McKay	Approved by DIGIT 14th February 2024
2.2	January 24	M. Corkery	Comments made
2.3	March 2024	Corporate Clinical Policy Group	Approved subject to minor amendments and final chair approval
2.4	March 2024	J. McKay	Amendments completed
3.0	April 2024	J. Cheung	Approved by chair action

Equality impact assessment

Consider if this document impacts/potentially impacts:

- Staff
- Patients
- Family members
- Carers
- Communities

Yes ☒ **complete box A**	**No** □ **complete box B**
Box A Contact the Trust's equality & inclusion manager at: **Email: ruth.besford@nhs.net** **Date contacted: 15/12/21**	**Box B** Complete details below: **Name:** **Email:** **Date:**

Education & Professional Development Question

In order to ensure that any training requirements are discussed, and resources planned and allocated to meet the needs of the service, you must consider whether this document has additional training requirements. Please answer the following question by entering a cross in the box below:

	Yes	**No**
Does this document have any additional training requirements or implications?		x

This table below must be completed in full for audit and governance purposes. Please note documents will be returned if section 1 in the table below is not completed fully. This will result in a delay in listing the document for approval.

Name of document	Records Management – Storing and Movement of Records Policy
Document number	IG/Pol/013
Document author	Jackie McKay
Section 1 - actions required by author	**Authors response**
Date proposal form submitted to policy officer (new documents)	16/1/24
Date proposal form presented to CCPG (new documents)	N/A
Date proposal approved by CCPG (new documents)	N/A
Date literature search/reference review requested	Completed by author March 2024
Date EqIA considered	N/A
Date additional training requirements considered	N/A
Date fraud-proofed by the Anti-Fraud Specialist (AFS) if applicable	16/1/24
Date template accessed on the Hub Add 'OFFICIALSENSITIVE: COMMERCIAL' to front cover if the document can be shared on the internet Add 'OFFICIALSENSITIVE: PERSONAL' to appendices if they include or will include personally identifiable information (PID)	January 24
Date literature review completed (check references are formatted correctly, and hyperlinks working)	March 2024
Date first draft submitted to policy officer for initial review	16/01/24
Date returned by policy officer following initial review	16/01/24
Date submitted to key individuals/groups/subject matter experts for comments (add names and designations of responders to consultation table)	16/1/24
For clinical documents, date document submitted to consultation group for sign-off i.e., IPC, Medicines Management (this applies if the document contains medication or medical gases - update version control sheet to confirm sign-off)	n/a
Name of Recommending Committee/group	DIGIT
Date sent to Recommending Committee/group for sign-off	7 Feb 2024
Date signed-off by the Recommending Committee/group (update version control sheet once signed-off)	14th Feb 2024
Date submitted to policy officer for listing at CCPG	20 Feb 2024
Section 2 – for completion by the policy officer	
Date approved by CCPG	15th March 2024
The following policies require Board approval and must be submitted to Board following CCPG approval: • Risk Management Framework Policy • Health & Safety Policy • Policy and procedure for the production, approval and ratification of Trust-wide policies and procedures ("Policy for Policies") Date submitted for Board approval: Date approved by Board:	n/a

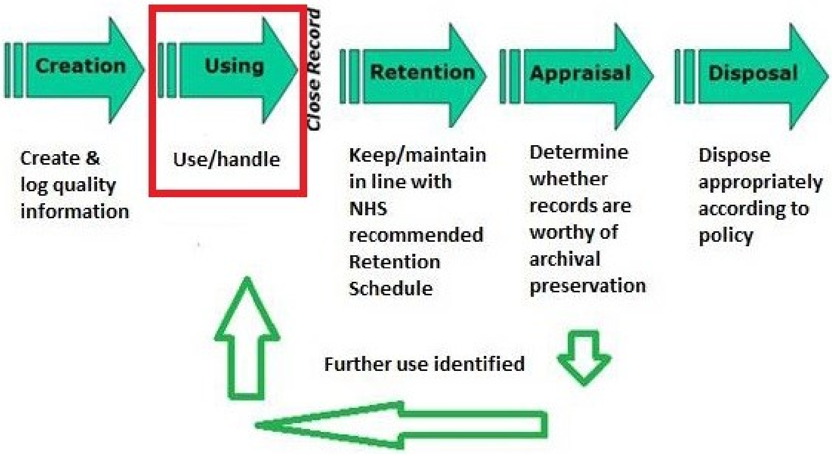
Contents

1 Introduction

This policy applies to all records (corporate and health records) paper or electronic, that are held by Bridgewater Community Healthcare NHS Foundation Trust (hereafter the Trust). The aim of this policy is to ensure uniformity across the Trust and to ensure that records management practice throughout the Trust complies with relevant legislation and national standards.

This policy sets out a framework for when a record has been created and is deemed “active” in “use” or being “handled” this includes storing and transferring the record.

Records/information Lifecycle – figure 1.


Creation
Using
Close Record
Retention
Appraisal
Disposal
Create & log quality information
Use/handle
Keep/maintain in line with NHS recommended Retention Schedule
Determine whether records are worthy of archival preservation
Dispose appropriately according to policy
Further use identified

The Trust’s Health Records Policy and the Corporate Records (including Document Management) Policy deals with the creation and standards of record keeping. The Records Management - Archiving, Retention and Disposal Policy details when a record is deemed closed and the record needs to be retained and appraised before being disposed. Additional records management and information governance (IG) policies can be found in section 4.

This policy does not cover when a patient needs to be transferred or readmitted for additional care from our Trust to another care organisation. This is covered in the Transfer of Patients Policy this policy has specific documents to be completed when a patient meets this criterion.

1.1 Objective

To ensure staff responsible for implementing this policy, have a robust framework to enable them to develop Local Non-Clinical Standard Operating Procedures (LNCSOPs) within each of their service. Each service needs to evidence an audit trail for all records held.

1.2 Scope

This policy is applicable to all personnel working, commissioned, or acting on behalf of the Trust including agency, locum, bank workers and learners in practice. This policy sets a standard framework for those who have been delegated responsibility for records management within the Trust.

2 Definitions

The definitions applicable to this document are as follows:

Caldicott Guardian	A Caldicott Guardian is a senior person responsible for protecting the confidentiality of people's health and care information and making sure it is used properly. All NHS organisations and local authorities which provide health and or social services must have a Caldicott Guardian.
Caldicott Principles	The Caldicott Principles (National Data Guardian (NDG) 22-23) are primarily intended to guide organisations and their staff when sharing patients, service users and/or their representatives' personal information. Good information sharing is essential for providing safe and effective care.
Classification of record	All records, whether they are held, electronically or in paper form, must be classified as a minimum as the following: • NHS Confidential • NHS Protect • NHS Public
Data security and protection toolkit (DSPT)	This is an online self-assessment tool that allows organisations to measure their performance against the National Data Guardian's 10 data security standards.
Freedom of Information (FOI)	FOI Act 2000 give the public's legal right of access to information held by government agencies and public authorities FOI Act 2000.
Health record	A health record has the classification of confidential. It consists of any information relating to the physical or mental condition of an individual and/or has been made by or on behalf of a health professional in connection with the care of that individual. Regardless of the format this can include: • Laboratory reports • X-ray and imaging reports • Photographs, slides etc. • Scanned information

	• Emails/text messages/message books • Correspondence for example a referral letter • Monitoring equipment print outs • Diary entries in electronic or paper format. A health record can also be called, patient record, case notes or medical record.
Incident reporting	An event or circumstance occurring in an NHS funded service that could have resulted, or did result in: 1. Unnecessary damage or loss to trust assets or reputation 2. Interruption to service delivery or trust objectives 3. Harm to patient, staff, visitors or members of the public.
Information asset owner (IAO)	Responsibilities of an IAO in managing the risks to personal information and business critical information held within a department. This includes approving, monitoring, and minimising data transfers.
Information governance (IG)	A framework which allows organisations and individuals to ensure that personal and corporate information is dealt with legally, securely, efficiently and effectively, in order to deliver the best possible care. It brings together all of the requirements, standards and best practice that apply to the handling of information.
NHS Counter Fraud Authority	The NHS Counter Fraud Authority (NHSCFA) is a special health authority tasked to lead the fight against fraud, bribery and corruption in the NHS. Focused entirely on counter fraud work, the NHSCFA is independent from other NHS bodies and is directly accountable to the Department of Health and Social Care.
Personal identifiable data (PID)	PID is data that contains sufficient information to be able to identify the specific person to whom the data belongs (patient or staff) e.g., name, date of birth, address. This generally excludes publicly available contact lists, such as staff telephone directories.
Record	Any record held by the NHS as a public body organisation, regardless of the media on which they are held. This includes health records, records of staff, complaints, corporate records and any other records held in any format, such as message books including both paper and digital records. The guidelines also apply to Adult, Social Care records where these are integrated with NHS patient records (NHS England 2022).

Retention	Records which are held before destruction to support reasonable, foreseeable litigation, Public Inquiries, and ongoing FOI request or similar exceptional statutory reasons, such as a public inquiry.
Special category data	The UK GDPR singles out some types of personal data as likely to be more sensitive, and gives them extra protection: • Personal data revealing racial or ethnic origin • Personal data revealing political opinions • Personal data revealing religious or philosophical beliefs • Personal data revealing trade union membership • Genetic data • Biometric data (where used for identification purposes) • Data concerning health • Data concerning a person's sex life; and • Data concerning a person's sexual orientation. In this guidance we refer to this as 'special category data.'
Tracer card	A tracer card is used to temporarily replace a paper record when it is removed from a filing system. The tracer card will contain the necessary details to locate the record should it not be returned.
Tracking and tracing log	A log which includes sufficient information including the date when the record was removed, by whom and reasons why. The log would then include when the record was returned.

3 Abbreviations

The abbreviations applicable to this document are as follows:

CCTV	Closed Circuit Television
CEO	Chief executive officer
CQC	Care Quality Commission
DPO	Data Protection Officer
DSPT	Data Security and Protection Toolkit
EPR	Electronic Patient Record
FOI	Freedom of Information
HR	Human Resources
IAO	Information Asset Owner
IG	Information Governance
IT	Information Technology
NHSCFA	NHS Counter Fraud Authority
LAC	Looked after Child

LNCSOP	Local Non-Clinical Standard Operating Procedures
NDG	National Data Guardian
NHS	National Health Service
PID	Personal Identifiable Data
RA	Registration Authority
SIRO	Senior Information Risk Owner
UKGDPR	United Kingdom General Data Protection Regulation

4 Other relevant procedural documents

This document should be read in conjunction with the following documents:

Acceptable Use (IT) Policy

Corporate Records (including Document Management) Policy

Data Protection and Confidentiality Policy

Disciplinary Policy and Procedure

Health Records Policy

Incident Reporting Policy

Information Asset & System Audit Policy

Information Governance Framework Policy

Information Security Policy

Information Technology (IT) Asset Management Policy

Looked After Children Policy

Mandatory Training and Induction Policy

Patient Identification Policy

Policy and Procedure for the Development and Review of Policy and Procedural Documents

Records Management, Archiving, Retention and Disposal Policy

Risk Management Framework

Subject Access/Access to Health Records Policy

Transition for Children to Adults Services Policy in Halton and Warrington

Transfer of Infants from Family Nurse Partnership Procedure

Transfer of Patients Policy

5 Roles and responsibilities

5.1 Chief executive officer

The chief executive officer (CEO) (accountable officer) has ultimate responsibility for the implementation of the provisions of this policy. The accountable officer is responsible for the management of the Trust and for ensuring that appropriate mechanisms are in place to support service delivery and continuity.

The Trust has a particular responsibility for ensuring that it corporately meets its legal responsibilities, and for the adoption of and compliance with internal and external governance requirements.

5.2 Chief nurse and deputy chief executive officer /Caldicott Guardian

The chief nurse/deputy CEO is the Trust Caldicott Guardian and is responsible for the confidentiality of person identifiable information as designated in the Caldicott Report and for the IG agenda which incorporates Data Protection legislation (Data Protection Act 2018), ensuring patient identifiable information is shared in an appropriate and secure manner according to the eight Caldicott Guardian principles (National Data Guardian (NDG) 22-23).

5.3 Director of finance/senior information risk owner

The director of finance/senior information risk owner (SIRO) is responsible for:

- Information risk throughout the organisation

- The overall ownership of the organisation’s Information Risks and risk management strategy and processes within the Trust

- Advising the Board on the effectiveness of information risk management across the Trust

- Providing an essential role in ensuring that identified information security risks are followed up and incidents managed.

5.4 Data protection officer

The data protection officer (DPO) is currently the Trust secretary.

The DPO has responsibility to ensure that the company or organisation is correctly protecting individuals’ personal data according to current legislation.

The DPO must have expert knowledge of data protection law and practices and the ability to acquire detailed understanding of the Trust's business, the purposes for which it processes, or intends to process personal data.

5.5 Information governance and records manager

The IG and records manager is responsible for:

- Ensuring the Trust is working within the legal frameworks in relation to handling information, specifically focusing on Data Protection.
- Ensuring this policy is implemented
- Ensuring the records management system and robust data quality processes are developed, co-ordinated and monitored
- Advising staff on records management issues.

5.6 Associate borough directors, assistant directors of operations, heads of Corporate Services, operational managers, and service managers

Associate borough directors, assistant directors of operations, heads of Corporate Services, operational managers and service managers will be accountable for ensuring that all corporate policies, procedures, and guidelines are fully implemented and approved within their directorate. This includes the responsibility for health records management outlined in the policy, making them the accountable record managers.

5.7 Heads of service/managers/team leaders

Heads of service/managers/team leaders are responsible for ensuring this policy is implemented across their area of their managerial responsibility and ensure that:

- Their staff are aware of and comply with this policy
- There is a service local-non clinical standard operating procedure (LNCSOP) to support this policy
- A designated person is appointed for each location to ensure archiving is managed appropriately
- Staff are aware of the location of policies, procedures and guidelines on MyBridgewater and that this information is given to all new staff on induction.

5.8 Staff

All staff has a duty to read and work within agreed policies, procedures and guidelines and to ensure that they keep themselves up to date with all procedural documentation. Staff must also ensure they are:

- Aware of the location of procedural documents and how to access them on MyBridgewater

- Compliant with their mandatory annual Data Security Awareness Level 1 training.

5.9 Digital, Information Governance and Information Technology Group

The Digital Information Governance and Information Technology Group (DIGIT) ensures the Trust operates within the IG framework and monitors compliance with this policy regarding corporate records.

6 Equipment

Not applicable.

7 Record management

The management requirement of a record is governed by its classification. The classification of a record is based on why the record is being created and for what purpose it will serve. A health or staff record for example is classified as confidential as they can contain both special category and personal information.

The standards for the creation, classification and naming of a record can be found in the Corporate Records (including Document Management) Policy; additional standards relating to a health record can be found in the Health Records Policy.

A service may have various record types each classified differently, with each being created and accessed differently. A record that is deemed confidential or private is to have stringent security controls this includes storing, handling (moving record from place to place within the Trust) and includes when a record needs to be transferred out of the Trust.

A record, files, notes, or other correspondence containing business or person identifiable information must be kept secure and handled with extreme care when it is being transported.

This policy mainly covers when a record has been classified as confidential or private and therefore needs to be controlled, but it is good practice to adopt the control measures for other records management outside of this remit. An example of this is when record that is classified as public; this document should be controlled whilst being developed, but once made public, this will not need to be controlled.

Once a record is created it needs to be managed through its life cycle. An audit trail for who has accessed, amended the record, any movement of the record needs to be tracked to enable the record to be traced and as up to date at any point.

Records, files, notes, or other correspondence containing business or person identifiable information must be stored in a secure location when not in use. This location needs to be secure with proper environmental controls and adequate protection against fire and flood. The Caldicott Principles must be applied, i.e., a record is only to be seen by those who need to see it.

The movement and location of records must be controlled to ensure that records can be retrieved at any time, and there is an auditable trail of record transactions. All records, files, notes, or other correspondence containing business or person identifiable information removed or borrowed from their store must be immediately and accurately tracked.

Should a record, file, notes, or other correspondence containing business or person identifiable information be identified as missing or lost, services need to define within their LNCSOP what requirements/efforts have been made before a record is deemed missing/lost, and an incident is to be raised and an investigation commenced. The outcome of the investigation and any lessons learned should be shared with the appropriate teams/people in the Trust.

8 Children's records

Tracking and tracing of records in an out of the organisations is to be maintained and recorded, this can be done on the electronic patient record (EPR) system. Records are only transferred when it is confirmed the child resides within that area.

All preschool (aged 5 and under) and safeguarding records are to be transferred as complete as possible, i.e., EPR and historical record (if one exists). It is acceptable to send the EPR record via email stating the historical record will follow.

If school children records (5 to 16) of universal children are being transferred, this should be done in electronic format only if there is a historical record on site; this should also be transferred. Note: Where there is a historical record in storage, this should be stated on the transfer information, but is only to be sent on request i.e., pulled out of storage.

Furthermore, when a child changes high school or district (when aged less than 16) a record or copy must also be transferred but only when the receiving authority has confirmed that the child is resident there. Failure to carry this out properly will mean many misplaced records will reside with the wrong child health or school nursing service. Those children who have left high school i.e., those in Year 11 records do not need to be transferred, unless specifically requested from the further education establishment.

It is the practitioner’s responsibility to ensure the receiving practitioner has sufficient information to deliver the care. All records that are requested for a transfer out, including safeguarding and LAC teams need to have the relevant electronic form completed by the responsible clinician.

The Trust will only accept records (movements in) of universal children in an electronic format.

Paper records that are received from a different organisation have to accepted and managed NHS Records Management Code of Practice (2023).

When a child moves to a different borough within the Trust, staff should limit the movement and the printing of the records. All movements of records (including copies) need be tracked and traced (see section 10 below).

9 Storage of records

Paper records, files, notes, or other correspondence containing person identifiable information need to be locked away in lockable filing cabinets/cupboards, with limited or monitored access i.e., via key fob. Rooms/buildings must be locked and/or alarmed when out of normal working hours. The location needs to be secure with proper environmental controls and adequate protection against fire and flood.

Electronic records need to be stored on information security controlled servers details (see the Information Security Policy); Staff must not save records on their personal drive, as some information may need to be accessed by other nominated team members in their absence.

Where a child’s record is stored on a school premises, access must be restricted to the health staff delivering care unless there is another lawful basis to access the record and a risk assessment completed.

Staff must not use their own personal mobile electronic devices to store personal identifiable information.

Staff who use electronic Trust devices to record or store records, files, notes, or other correspondence containing business or person identifiable information, must follow the Information Security Policy.

10 Tracking and tracing of records

The tracking and tracing of records, files, notes, or other correspondence containing business or person identifiable information is the responsibility of all staff involved in the handling of these records. Stored records may potentially be required by the Anti-Fraud Specialist to support the conduct of criminal investigations.

Records need to be monitored to ensure they are available for continuity of care or an appropriate investigation. All records, files, notes, or other correspondence containing business or person identifiable information removed/borrowed from their store must be immediately tracked using a tracer system. This includes those service that use a combination of electronic and paper records.

A risk assessment of record management processes should be reviewed as a minimum yearly or when a change of practice has occurred.

There are different types of tracer systems that should be adopted (examples below). The tracking system is to include the following details as a minimum:

- Unique identifier (NHS number etc.)
- Name of patient/staff record identifier
- The destination – e.g., contact details of the person, unit, service or department to whom the record is being sent
- Date sent
- Sign and date the tracer card.

Here are three examples of tracer systems that could be adopted for an LNCSOP to be developed:

1. <u>Use of Tracer card system</u>

- Locate the health record which is required
- Insert a tracer card in place of the health record which is being removed
- Include the minimum details above
- Once the record is returned the tracer system is updated.

2. <u>Use of register</u>

For those services that are not able to use tracer cards they must operate and maintain a register by using a book, diary, Excel spreadsheet or database saved on secure server or index card to record transfers:

- Locate the record which is required
- Record entry in register
- Include the minimum details above
- Once the record is returned the tracer system is updated.

3. Electronic tracking system

Where a shared electronic tracking system is operated as part of an information system:

- Locate the record which is required

- Request the record by selecting the organisation and service point that requires the record

- Dispatch the requested record to the requested location

- Receiver of record to entry on electronic system which will automatically update current location and service point.

11 Physical transportation of records

Transfers or transportation of more than 50 health records must be preauthorised by the Caldicott Guardian, as this constitutes a ‘bulk data transfer’. This only applies outside of the archiving process (to an offsite storage company) for example, when a service moves premises. Staff need to seek advice from the IG team for details.

Once staff have tracked the record or any data or records containing business or person identifiable information, it is imperative they are transported securely.

- Records, files, notes, or other correspondence containing business or person identifiable information must be transferred using appropriate trolleys, sealed box, sealed envelope, zipped pouch or locked cases/carriers and never be deposited and left unattended in areas that are not secure e.g., entrances, corridors, stairways or in vehicles where the package is visible, or the vehicle unlocked.

- During working hours any records, files, notes or other correspondence containing business or person identifiable information must be stored in a locked carrier locked in the van or car boot.

- When visiting a patient or staff member in the community only the relevant paperwork should be removed from the vehicle. All other paperwork must remain in a locked carrier and locked and out of sight in the boot.

- Outside working hours, the best practice is to return, files, notes or other correspondence in paper form at the end of the day to the base location. However, it is recognised that this is not always practical. If data or records cannot be returned, they should be taken into the staff member's home in a locked carrier and stored safely and securely preventing inappropriate access to the files.

- Paper records must not be taken into a public place such as a shop or café. This does not apply to an electronic device such as a mobile phone.

- If staff require to take paper records, files, notes, or other correspondence containing business or person identifiable information outside their base location in order to perform their duties, this should be subject to a risk assessment and approval by the appropriate line manager to ensuring data protection, Caldicott, and Trust policies are followed.

- Paper records or information technology (IT) equipment must never be left in a car overnight.

12 Consultation

Key individuals/groups involved in the development of the document to ensure it is fit for purpose once approved.

Name	Designation
Mary Corkery	Policy Officer
Ruth Besford	Equality and Inclusion Manager
DIGIT	Director of Finance/SIRO Associate Director of Halton Adult Community Services Deputy Director of Finance Programme Manager Digital Training Manager and Registration Authority Lead (Access Control)
Phillip Leong	Anti-Fraud Specialist
Jillian Wallis	Associate Director
Karen Worthington	Associate Director for Children’s Services
Debbie Greenall	Dental Services Manager
Katherine Summers	Infection Prevention and Control Lead Nurse
Corporate Clinical Policy Group	

13 Dissemination and implementation

13.1 Dissemination

This policy will be disseminated via the IG and records manager to associate borough directors and assistant directors of operations for disseminating to staff.

The policy will be made available on the extranet and published in the team brief, information governance newsletter and a link made available on the records management bespoke extranet page.

13.2 Implementation

All Trust staff will be made aware of their personal and organisational responsibilities regarding handling of NHS confidential records, through the Trust training program, and local induction and monitoring audits. New employees will be made aware of this policy through the local Induction process.

14 Process for monitoring compliance and effectiveness

Process for reviewing compliance and effectiveness i.e., audit, review, survey, incident reporting	Responsible	Frequency of monitoring	Assurance Group
DSPT	SIRO	Annual	DIGIT

As requirements contained in this policy form one part of regulative requirements, for example Care Quality Commission (CQC) and professional bodies, failure to comply will be seen as an incident and upon investigation may lead to disciplinary and/or legal action in line with Human Resources (HR) policies and procedures by the Trust.

15 Standards/key performance indicators

Key performance indicator	Evidence required	Frequency	Committee/ person responsible
Monitoring of incidents or issues raised relating to aspects in this policy	Report	Quarterly	IG

16 References

Data Protection Act 2018, c.12 [online]. Available at: http://www.legislation.gov.uk/ukpga/2018/12/contents

National Data Guardian (2024) National Data Guardian 2022-2023 report. [online] Available at: https://www.gov.uk/government/publications/national-data-guardian-2022-2023-report/national-data-guardian-2022-2023-report

Freedom of Information Act 2000. [online]. Available at: https://www.legislation.gov.uk/ukpga/2000/36/contents

NHS Digital. (n.d.) (webpage) Data Security and Protection Toolkit assessment guides 2023-2024 (version 6 standard) [online]. Available at: https://digital.nhs.uk/cyber-and-data-security/guidance-and-assurance/data-security-and-protection-toolkit-assessment-guides.

NHS Digital (2021) Data Security and Protection Toolkit [online]. Available at: https://www.dsptoolkit.nhs.uk/

NHS England (2014) National health visiting service specification 2014/15 [online]. Available at: https://www.england.nhs.uk/wp-content/uploads/2014/03/hv-serv-spec.pdf

NHSx (2021) Records management code of practice for health and social care [online]. Available at: https://www.nhsx.nhs.uk/information-governance/guidance/records-management-code/

NHS England (2022) High quality patient records. [online] Available at: https://www.england.nhs.uk/long-read/high-quality-patient-records/.

Public Health England (2015) Child health information systems: information requirements and output specifications. [online] Available at: https://www.gov.uk/government/publications/child-health-information-systems-information-requirements-and-output-specifications

Public Health England (2015) Output and information requirements specification: for the Child Health information service and systems, (PHE publications gateway number: 2014824) [online]. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/417076/Child_Health_Information_240315.pdf