Information Lifecycle Policy  
(Records Management)  
Version: 5

Summary: This document defines Trust policy with regard to information and records management in line with GDPR/DPA 2018, CQC, NHSLA CNST, Data Security & Protection Toolkit requirements and NHS Records Management Code of Practice 2016.

Keywords (minimum of 5): Information; records; management; retention; disposal; electronic; emails; corporate records; creation;

Target Audience: Southern Health NHS Foundation Trust employees, Non-Executive Directors and Contractors.

Next Review Date: 3 years, September 2020

Approved and ratified by: Information Governance Group  
Date of meeting: 11/09/2017

Date issued: September 2017

Author: Lesley Barrington - Head of Information Assurance

Accountable Director: Paula Anderson, Finance Director
## Version Control

### Change Record

<table>
<thead>
<tr>
<th>Date</th>
<th>Author</th>
<th>Version</th>
<th>Page</th>
<th>Reason for Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>09/08/2011</td>
<td>L Barrington</td>
<td>V1</td>
<td>All</td>
<td>Review and combination of previously HPFT &amp; HCHC policies and procedures</td>
</tr>
<tr>
<td>08/08/2012</td>
<td>R Gray</td>
<td>V2</td>
<td>All</td>
<td>Add Equality Impact Assessment Screening Tool</td>
</tr>
<tr>
<td>17/09/2012</td>
<td>RG</td>
<td>V2</td>
<td>9</td>
<td>Update section 10: to include ‘and sender on reverse’.</td>
</tr>
<tr>
<td>24/06/2015</td>
<td>L Barrington</td>
<td>V3</td>
<td>All</td>
<td>Update and review Update regarding the change to the Public Records Act – 20 year rule for retention of corporate records.</td>
</tr>
<tr>
<td>May 2017</td>
<td>L Bega</td>
<td>V4</td>
<td>All</td>
<td>Merging of SH IG 02 Access, movement &amp; storage of clinical records procedure, SH IG 04 Creating and Managing a Clinical Record Procedure, SH IG 03 Mislaid or Lost Clinical Records Procedure with SH IG 13 Information Lifecycle Policy and SH IG 15 Managing Documents – Guidance and Standards</td>
</tr>
<tr>
<td>June 2018</td>
<td>L Barrington</td>
<td>V5</td>
<td>All</td>
<td>Pages reviewed to reference General Data Protection Regulation / Data Protection Act 2018 Updated Accountable Director on front cover</td>
</tr>
<tr>
<td>April 2019</td>
<td>D Woolley</td>
<td>V5</td>
<td>13</td>
<td>Legacy name change: generic email from HP-TR. To SHFT</td>
</tr>
</tbody>
</table>

### Reviewers/contributors

<table>
<thead>
<tr>
<th>Name</th>
<th>Position</th>
<th>Version Reviewed &amp; Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGG Membership</td>
<td></td>
<td>V1 2011</td>
</tr>
<tr>
<td>CIASG members</td>
<td></td>
<td>V2 d0.3 8.8.12</td>
</tr>
<tr>
<td>IGG</td>
<td>IG Leads and Members</td>
<td>V3 13/07/2015</td>
</tr>
</tbody>
</table>
# Contents

<table>
<thead>
<tr>
<th></th>
<th>Introduction &amp; Design and Implementation of Record Keeping Systems (DIRKS)</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.</td>
<td>Who does this policy apply to?</td>
<td>5</td>
</tr>
<tr>
<td>3.</td>
<td>Definitions</td>
<td>5</td>
</tr>
<tr>
<td>4.</td>
<td>Duties / Responsibilities</td>
<td>6</td>
</tr>
<tr>
<td>5.</td>
<td>Main Policy Content</td>
<td>7</td>
</tr>
<tr>
<td>5.1</td>
<td>Record Creation</td>
<td>8</td>
</tr>
<tr>
<td>5.2</td>
<td>Protective Marking</td>
<td>8</td>
</tr>
<tr>
<td>5.3</td>
<td>Naming Files – Rules</td>
<td>10</td>
</tr>
<tr>
<td>5.4</td>
<td>Naming Folders</td>
<td>10</td>
</tr>
<tr>
<td>5.5</td>
<td>File Properties</td>
<td>11</td>
</tr>
<tr>
<td>5.6</td>
<td>Quality and Accessibility</td>
<td>11</td>
</tr>
<tr>
<td>5.7</td>
<td>Security, Storage and Retrieval</td>
<td>12</td>
</tr>
<tr>
<td>5.8</td>
<td>Misplaced or Lost Records</td>
<td>12</td>
</tr>
<tr>
<td>5.9</td>
<td>Transport and Transfer of Information</td>
<td>14</td>
</tr>
<tr>
<td>5.10</td>
<td>Information Asset Register and Data Protection Act Compliance</td>
<td>15</td>
</tr>
<tr>
<td>5.11</td>
<td>NHS Code of Practice: Records Management – Records Inventory</td>
<td>15</td>
</tr>
<tr>
<td>6.</td>
<td>Training Requirements</td>
<td>16</td>
</tr>
<tr>
<td>7.</td>
<td>Monitoring Compliance</td>
<td>16</td>
</tr>
<tr>
<td>8.</td>
<td>Policy Review</td>
<td>16</td>
</tr>
<tr>
<td>9.</td>
<td>Associated Documents</td>
<td>16</td>
</tr>
<tr>
<td>10.</td>
<td>Supporting References</td>
<td>16</td>
</tr>
<tr>
<td></td>
<td>Appendix 1</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td>Appendix 2</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td>Appendix 3</td>
<td>19</td>
</tr>
<tr>
<td></td>
<td>Appendix 4</td>
<td>20</td>
</tr>
</tbody>
</table>
1. **Introduction**

All NHS records (including email and electronic documents) are public records under the terms of the Public Records Act 1958; sections 3 (1)–(2) and must be kept in accordance with the following statutory and NHS guidelines:

- The Public Records Act 1958 and 1967
- The General Data Protection Regulation / Data Protection Act 2018
- The Freedom of Information Act 2000
- The Common Law Duty of Confidentiality
- NHS Code of Practice: Confidentiality

All NHS records are public records under the terms of the Public Records Act 1958. “The 20 Year Rule” is being implemented in the NHS by the National Archives. This change to the Public Records Act 1958 supports key government policies around transparency, accountability and recommendations from the Francis report into Mid Staffordshire. It will affect the timing of transfer of records of historical value to The National Archives or other public archive services, which will take place ten years earlier than at present. The local place of deposit (POD) is the Records Office in Winchester. Refer to SH IG 16 Records Retention, Archiving and Disposal Procedure for more information.

Guidance on the management of NHS records is provided by the Department of Health in the Records Management: NHS Code of Practice which sets out a schedule of minimum retention periods for many types of record and is based on legal requirements and professional best practice. This policy adopts the retention and review guidance in that document.

Information is a corporate asset. Southern Health NHS Foundation Trust (the Trust) and its legacy organisations records are its corporate memory, providing evidence to actions and decisions and representing a vital asset to support daily functions and operations. Records support policy formation and managerial decision-making, protect the interests of the Trust and the rights of patients, staff and members of the public. They support consistency, continuity, efficiency and productivity and help deliver services in consistent and equitable ways.

The organisational benefits of sound records management are:

- control and availability of valuable information assets
- efficient use of staff time
- compliance with legislation and standards
- good utilisation of storage and server space
- reduced costs
- support for the day to day business that underpins delivery of healthcare
- decision making
- continuity of healthcare provision
- effective and timely communication of care needs
- clinical effectiveness and evidence based clinical practice
- legal requirements
- monitoring and audit
Records must be available whenever and wherever there is a justified need for information and in whatever media required.

The Trust has a responsibility to ensure that the healthcare each patient receives is recorded appropriately and that records are processed responsibly to support high quality care. There are professional standards for clinical record-keeping which are part of the requirements for professional registration. For legal and practical reasons records must be stored and transported securely.

2. **Who does this policy apply to?**

This policy applies to all staff who create and use records as part of the delivery of Trust business. This covers all records in all formats (paper and electronic), both active and inactive, held for use in the organisation, including:

- administrative (e.g. corporate, provider services, contracts and commissioning, personnel, estates, finance and accounting, customer services and litigation) including e-mails and text messages

- clinical, including Out-of-Hours GP Services and all patients seen privately or under contract to the NHS on NHS premises, reports (including paper, microfilm/microfiche, x-rays and other imaging, video and audio tapes and all electronic records.) [See detail for clinical records in Clinical Information Assurance (Record Keeping) Policy and associated guidelines and procedures]

This policy excludes:

- copies of documents created by other organisations such as the Department of Health, kept for reference and information only

- patient records held by independent practitioners i.e. GPs, Dentists, Pharmacists and Optometrists

Hospital case notes are shared across local health economies and managed by acute hospital trusts under Service Level Agreements. The Trust will adhere to filing and records policies and procedures ratified by these trusts when using these records. Likewise appropriate external procedures will be followed when handling records transferred from any other NHS Trust.

3. **Definitions**

Records management is a discipline which utilises an administrative system to direct and control the creation, version control, distribution, filing, retention, storage and disposal of records, in a way that is administratively and legally sound, whilst at the same time serving the operational needs of the Trust and preserving an appropriate historical record. The key components of records management are:

- creation
- quality and accessibility
- standards and maintenance systems
- disclosure and information sharing
- transfer and tracking of movements
- storage
• culling/reviewing, closure
• retention
• archiving
• disposal

The term records lifecycle describes the life of a record from its creation/receipt through the period of its “active” use, then into a period of “inactive” retention (such as closed files which may still be referred to occasionally) and finally either confidential disposal or archival preservation.

In this policy, records are defined as “a recorded document which forms part of a structured file that contains information, in any medium (including electronic, audio, visual, microfiche), created or received and maintained by the Trust in the transaction of its business or conduct of affairs and kept as evidence of such activity”.

Records may also be referred to as files. For electronic files, this refers to files created and/or amended using Microsoft Word, Excel, PowerPoint, Publisher plus any other software packages, including Electronic Patient Records (e.g. RiO). The Windows definition of a file is a “complete, named collection of information, such as a program or user-created document”. In short, a file is a basic unit of storage that enables a computer to distinguish one set of information from another. It is a collection of data that a user can retrieve, change, delete, save or send to an output device, such as a printer or email program. Windows uses folders to provide a storage system for files on a computer, just as manila folders might be used to organise paper information in a filing cabinet.

When handling any type of record, it is important to make the distinction between a record and a document. A document becomes a record when it has been finalised and become part of the record inventory (corporate) or clinical record (patient).

4. Duties / Responsibilities

The Trust has a legal responsibility to ensure that all its clinical, administrative and corporate staff keep proper records.

All Trust staff, whether clinical or administrative, are responsible for any records they create, receive and use and are responsible for adhering to the Trust’s policies and procedures in relation to records management. Registered professionals are responsible for complying with their relevant codes and standards of professional practice.

The Chief Executive has overall responsibility for records management in the Trust. As the accountable officer he/she is responsible for the management of the organisation and for ensuring appropriate mechanisms are in place to support service delivery and continuity. Records management is key in ensuring appropriate, accurate information is available as required.

Divisional and Corporate Directors; Area, Locality and Departmental/Services Managers have responsibility for records generated within their departments and for ensuring that their staff undertake the training provided; are aware of the requirements of this policy and apply the correct procedures and controls.

The Caldicott Guardian is responsible for ensuring that Caldicott principles are followed:
• the purpose of using confidential information must be justified;
• confidential information must only be used when absolutely necessary;
• the minimum information necessary to achieve the purpose should be used;
• access to confidential information must be on a strict need-to-know basis;
• everyone accessing confidential information must understand his or her responsibilities;
• everyone accessing confidential information must comply with the law.
• Information should be shared appropriately in order to provide integrated care.

The Senior Information Risk Officer (SIRO) has ultimate responsibility for the management and mitigation of risks associated with the Trust’s information management processes.

The Lead for Freedom of Information (FOI) is responsible for administering all requests for information made to the Trust. The Lead for FOI will also provide a point of contact for all members of staff who require advice on freedom of information act matters.

The Head of Information Assurance and Information Governance Manager are responsible for the implementation of this policy through the Information Governance Strategy and Information Governance Group and framework, which includes training and audit.

The Records Manager is responsible for the overall development and maintenance of records management processes throughout the Trust, including overall management of contracts with off-site storage providers, and the maintenance of corporate inventories.

Information Asset Owners and Administrators are responsible for ensuring that all information assets are managed appropriately. Refer to the Information Governance Policy and Framework for more information.

5. Main policy content

The aims of the policy are to ensure:

• Accountability – Records are adequate to account fully and transparently for all actions and decisions, in particular to:
  o protect legal and other rights of staff or those affected by those actions;
  o facilitate audit or examination;
  o provide credible and authoritative evidence.

• Availability – Records are available when needed and the Trust is able to service its business needs and comply with legislative requirements.

• Accessibility – Records can be located when needed and only those with a legitimate right can access the records and the information within them is displayed in a way consistent with its initial use, and the current version is identified where multiple versions exist.

• Interpretation - The context of the record can be interpreted i.e. identification of staff who created or added to the record and when, during which business process, and how the record is related to other records.

• Quality – Records can be trusted - are complete and accurate and reliably represent the information that was actually used in, or created by, the business process, and its integrity and authenticity can be demonstrated.
- **Maintenance through time** - so that 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.

- **Security** – Records are secure from unauthorised or inadvertent alteration or erasure, access and disclosure are properly controlled and there are audit trails to track all use and changes in order to ensure that records are held in a robust format which remains readable for as long as records are required.

- **Retention and disposal** – Records are retained and disposed of appropriately, using consistent and documented retention and disposal procedures, which include provision for appraisal and the permanent preservation of records with archival value.

- **Staff are trained** – so that all staff are made aware of their responsibilities regarding records management.

5.1 **Record creation**

All electronic and paper records must conform to the Trusts specifications for referencing, version control, naming, filing and filing structures, and be for a legitimate clinical or business process.

It is important that all files are managed in accordance with the relevant Trust policies and procedures. **Every member of staff is responsible for the management of the files they create (including those they access and modify).**

When creating new files such as spreadsheets, word processed files, discrete databases or presentations it is important to consider if there is a business need for the file. **All files which relate in any way to official business fall within the definition of public records under the Public Records Act 1958 and 1967 and may be disclosable under FOI.**

When using Word, file markings can be inserted as watermarks (e.g. Draft, Confidential, Version 01 etc.) or via the file header and/or footer function. [See the Microsoft “help” function for detail]

For Clinical Records and Electronic Patient Records - please also refer to the Record Keeping Policy SH IG 01 and associated documents and to the appropriate Standard Operating Procedure or Handbook.

5.2 **Protective marking**

Protective marking denotes how a document should be treated, this affects how a document is saved, stored, transferred and whether it may be disclosed.

File markings reflect the level of confidentiality the file should have. 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 make appropriate decisions about distribution and storage.

File markings can be set by the author of a file to ensure that other members of staff are informed of the status of the file. However, such markings will not prevent disclosure of the record under FOI, unless an exemption applies. As a general rule the following classifications for confidential files may be used:
### Naming conventions

The Trust follows advice issued by the National Archives, i.e:

- Give a unique name to each document.
- Give a meaningful name which closely reflects the record contents.
- Express elements of the name in a structured and predictable order.
- Keep file and folder names as short as possible.
- Locate the most specific information at the beginning of the name and most general at the end.

Files/documents should be named using the following convention:

- **Document title–Date-Version number**

  The date should be in the format `yyyymmdd` (e.g. 2018 01 01)

Version indicators help to keep track of the development of a file. The format recommended is to use the ordinal number (1, 2, 3, etc.) for major version changes and decimal numbers (e.g. 0.1, 0.2) for minor changes. All drafts should have version numbers less than 1.0 (e.g. 0.4).

### Document types and suggested abbreviations:

<table>
<thead>
<tr>
<th>Type</th>
<th>Abbreviation</th>
<th>Type</th>
<th>Abbreviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action Plan</td>
<td>Act</td>
<td>Plan</td>
<td>Pln</td>
</tr>
<tr>
<td>Agenda</td>
<td>Ag</td>
<td>Policy</td>
<td>Pol</td>
</tr>
<tr>
<td>Audit</td>
<td>Aud</td>
<td>Presentation</td>
<td>Pres</td>
</tr>
<tr>
<td>Briefing</td>
<td>Brf</td>
<td>Procedure</td>
<td>Proc</td>
</tr>
</tbody>
</table>

---

**Classification | Saving | Storage | Disclosure**
--- | --- | --- | ---
**Strictly Confidential** | Limited access (personal or restricted drive) | Locked cabinet, locked room | Exempt from public disclosure under FOI. Exempt from personal disclosure under DPA. |
**Confidential** | Limited access (personal or restricted access drive) | Locked cabinet, locked room | Exempt from full disclosure under FOI, but may be disclosable under DPA. |
**Private and Confidential** | Limited access (personal or restricted access drive) | Locked cabinet, locked room | Exempt from full disclosure under FOI, but may be disclosable under DPA. |
**Personal & Confidential** | Personal drive | Locked cabinet, locked room | Exempt under FOI. Disclosable to the individual under the DPA. |
**Sensitive** (includes personal information of particularly private nature, commercially sensitive information) | Limited access (personal or restricted access drive) | Locked cabinet, locked room | May be currently exempt under FOI but disclosable at a later date. Disclosable to the individual under DPA (unless exempt) |
5.3 Naming files – rules:

1. **Keep file names short, but meaningful.** Long file names mean long file paths which increase the likelihood of error, are more difficult to remember and recognise, and are more difficult to transmit in emails. However, avoid using initials, abbreviations and codes that are not commonly used.

2. **Avoid unnecessary repetition.** As above.

3. **Use capital letters to delimit words, not spaces or underscores.** Some software packages have difficulty recognising file names with spaces. Instead of spaces and underscores, use Capitals to separate words.

4. **If using a number in a file name – use two digits.** Unless it is a year or a number with more than two digits.

5. **If using a date in a file name – use YYYYMMDD.** This will ensure that in a list of files in a folder, the most recent is always at the bottom.

6. **Using personal names.** This is usually used in filing correspondence. Use surname first, and then initial and the date as above. This will ensure that the correspondence will list in chronological order.

7. **Avoid using “draft” or “letter” at the start of names.** There may be several documents in draft in a folder and it will be easier to locate the right document if it is filed by its title. Once a document has been ratified, all draft versions must be deleted as these would remain subject to the Freedom of Information Act and/or the Data Protection Act.

When using Word and/or Excel, filenames and paths must always be displayed in the footer of the file. [See Microsoft Help for detail.]

5.4 Naming Folders

Naming principles are also applied to folders: ways in which this can be done include:

- Using standard terms for themes and activities
- Using consistent logical labels to describe business activities and functions
- Using a clear explanation of what a folder contains
- **People’s names for directory or folder names must not be used (job titles or roles are acceptable).**

In order to comply with Freedom of Information, the Trust requires a quick and easy way to find all files saved on Trust servers, and staff are required to complete the file properties box on all documents produced. This may be achieved through the use of the properties box within each application of Microsoft Office – Word, Excel, Access, Powerpoint, etc.
5.5 File Properties

Consistency in where files are saved contributes to making it easier to find files.

Files should be saved as follows:

- Files which are approved by the Trust Board and which are ready to be shared across the whole Trust are saved on the website/Staff Intranet. (Documents to be placed on the intranet must be referred to the Communications Team).

- Shared network drives are for files to be shared with colleagues. Shared or personal drives should not be used for the long-term storage of corporate level files, which should be made available to all staff via the Intranet.

- Saving files to personal drives is not allowed, as it restricts the Trust's ability to meet its legal obligations.

- The Trust requires staff to save their files to the shared network drive. If it is necessary to restrict access, raise a call with the IT Service Desk to create a new shared drive area with access restricted to designated named individuals. Ensure that the Service Desk is informed of leavers to be removed for access privileges, and new staff to be added.

- Files saved on personal drives should be restricted to files which do not need to be accessed by others and which will be exempt under the FOI and DPA.

**Staff must not save information to the local hard drives** on personal computers (i.e. ‘C’ Drives), in accordance with the Information Security Policy. Information on local hard drives is not backed up, therefore loss or damage to the PC will result in permanent loss of the information.

5.6 Quality and accessibility

To ensure quality and continuity of operational and corporate services, information is only useable if it is accurate, correctly and legibly recorded, kept up to date and easily accessible when needed.

To comply with the Data Protection Act principles, records should not be kept for longer than is necessary and therefore should be subject to review and archive or deletion at the expiry of their retention period.

Access to records, in any format, should be restricted to designated and authorised staff. Confidential paper records should be kept in a locked cupboard or locked filing cabinet, and the room should be locked when not in use.


Access to information via the Data Protection Act 2018 is covered in the Confidentiality and Data Protection Act Policy – and Access to Personal Records Procedure.
5.7 Security, storage and retrieval

For legal and practical reasons records should be stored securely until minimum retention periods have expired, but no longer than required to support the business needs of the organisation (as defined by the SH IG 16 Retention, Archiving and Disposal Procedure).

The Trust will comply with the seven Caldicott principles, which govern the access and use of confidential information, the NHS Confidentiality Code of Practice, and the requirements of the Data Protection Act 1998.

Staff who record, handle, store or otherwise come across personal information have a personal common-law duty of confidence. Unauthorised disclosure or misuse of information in records constitutes a breach of confidentiality and as such will lead to disciplinary action and could lead to dismissal. Refer to SH IG 18 Data Protection & Confidentiality Policy

To promote patient involvement and enable efficient information-sharing, community health records may be left in the patient’s home. Individual patients/parents are responsible for the custody of their own patient/parent-held records. Whenever records are held in the home, it is the responsibility of staff to convey to the patient/parent their responsibility to take care of these records, safeguard their confidentiality and return them at conclusion of treatment. These records remain the property of the Trust.

Hard copies of records must be kept secure and should be stored in an appropriate locked filing cabinet, office or designated records store on site, or in an approved off-site storage facility, so they are available and accessible to those who need them. Information retained must be in line with national guidance, the Data Protection Act 1998, the NHS Code of Practice, and ISO 15489/1:2001. Information retained electronically must be in line with the Data Protection Act 1998 and the NHS Code of Practice on Confidentiality. Also refer to SH IG 42 Procedure for the Management of Personal Information.

Records placed in storage, either on site or with an off-site storage company must comply with the SH IG 16 Archiving Guidelines and Procedure.

If a record cannot be located at its using place of residence – then section 5.5 ‘Mislaid or lost records’ must be followed.

5.8 Mislaid or lost records

A record is defined as “unavailable” if it is in use elsewhere and/or cannot be immediately located. A temporary record should be created, clearly marked as a temporary record, populated with all available relevant information from the available systems, and an entry should be made in the appropriate electronic system.

A tracer card should be put in the usual place of storage for the record – marked that a temporary file has been created, and its location. When the original records are located/returned, the temporary file must be combined with the original.

If a record is considered to be mislaid, missing or lost – the following procedure must be followed:

Immediate action:

- Highlight the fact that a record is 'missing' to your line manager and work colleagues.
- Search the place you would normally expect to find the record, and any other relevant locations Check what the tracer card or system (e.g. electronic record) says
Make a list of all the places that have already been searched and maintain this list as the search progresses in case an incident form needs to be completed if the records remain missing.

Check the above again 2 working days later as occasionally records reappear.

If the record isn’t found, complete an incident on Ulysses Safeguarding System

Clinical Records:

For inpatient services with no electronic record – if the notes have not been found within 2 working days - an Incident Form must be completed on the Safeguard Incident Reporting System and marked as “Lost or Stolen Paperwork” – detailing the action taken to date, and any planned action.

All other areas - In 10 working days (or prior to the next time they are required if sooner):

a) If the notes have not been traced within 10 working days or prior to the next time they are required for a consultation if sooner, an Incident Form must be completed on the Safeguard Incident Reporting System and marked as “Lost or Stolen Paperwork” – detailing the action taken to date, and any planned action.

b) In the event of a complete failure to locate the records, then a temporary folder should be raised, clearly marked as a “temporary folder”, and indicating who the original should be sent to (i.e. the member of staff who has been searching for the record) should it be located. If after 2 months the original has not been found – this file should be renamed “re-constituted” (see below). Where RiO is deployed – ensure that a progress note has been included that details action taken.

c) Inform the Information Assurance Team by means of a phone call, fax or email (shft.informationassuranceteam@nhs.net) if the original notes are found.

d) Should the clinical records be stolen and therefore have the potential to get into the public domain, the Trust has a responsibility to inform the patient and/or family. The Lead Healthcare Professional (HCP) must be consulted before any contact is made with the patient or family, before doing so to discuss their current mental and/or clinical needs and the most appropriate person to inform them of what has happened, to explain what the Trust is doing to recover the notes (if necessary) and what measures are being taken to prevent a recurrence.

Reconstituting records which have been inadvertently lost, damaged or permanently destroyed

If, despite the use of good tracer and tracking systems, a record is temporarily lost or mislaid, step i) above must be followed.

On the very rare occasions when the record has been inadvertently destroyed, it will be necessary to reconstitute the records to the best of the Trust’s ability. The following steps must be taken:

a) Ensure that a Safeguard incident form has been completed
b) Print off from any available electronic system or shared drive correspondence and other documentation (e.g. care plan);

c) If a clinical record, ask all clinicians who had any contact to re-create their manual record – stating that this is a reconstituted record and from memory;

d) Contact other agencies for copies of correspondence and communications which they had originated and copied to the Trust or received from the Trust.
e) Create a new records folder – and ensure that it is labelled “re-constituted”.
f) Lead Health Care Professional to inform the patient.

Contaminated records

a) Where the records or parts of the record have been contaminated, arrange for the relevant pages to be copied (if necessary, by putting them into plastic wallets).

b) Check that the photocopies contain all the information from the original record. If necessary, make good any entries which have been affected by the copying process.

c) Mark each page: ‘DUPLICATE. Original was contaminated and has been destroyed for clinical and safety reasons. See entry in records dated ........”.

d) Document in the record (paper and electronic patient record if appropriate) in the notes that x pages were contaminated on (date) by (reason) and that copies were taken and the originals destroyed. Arrange for the contaminated originals to be securely destroyed.

Monitoring and follow up action:

The Information Assurance Team will be informed by automatic message from the Safeguard Incident System when an incident is raised which identifies that a clinical record is mislaid/lost. A log of all such incidents will be maintained with details of actions taken, and will follow up with the services as required. This will be reported to the Information Governance Group on a quarterly basis to identify and monitor trends, and support changes to process/procedure as required to mitigate the risk of further losses.

5.9 Transport and transfer of information

Where information is to be transported or transferred, either within or to outside agencies, SH IG 42 Procedure for the Management of PID must be followed.

The lifecycle of a document shall be determined at point of creation and that all of the Trusts records are retained for a minimum period of time for legal, operational, research and safety reasons. This shall be in accordance with the retention periods set out in the Records Management: NHS Code of Practice 2016 to ensure that:

- time-expired records are reviewed promptly
- no records or part of records are destroyed which are subject of any known litigation, enquiry, Child Safeguarding proceedings or request (or appeal) for information under the Freedom of Information, Data Protection or Access to Health Records Acts;
- no current or non-time-expired records are destroyed;
- the method of destruction is secure and confidentiality is maintained at every stage. In practical terms this means shredding, pulping or incineration.
- there is adequate documentation of the disposal of records, including identification information, date and authority for disposal, disposal method and by whom carried out, confirmation that disposal/destruction has taken place;
- destruction of time-expired records stored commercially is authorised promptly and certification retained.

Records will be retained, reviewed and destroyed in accordance with the Retention, Review and Disposal schedule.

Options for the archiving of paper records include scanning to an alternative format (such as micro-film or CD-ROM), on-site or commercial storage, confidential destruction (by
shredding, pulping or incineration). Information of potential historic or research importance should be deposited with an organisation which wishes to carry on using it e.g. National Archives or bona fide research body.

Requests for extended preservation will be subject to approval by the Records Manager. Extended preservation may be advised on grounds of historical archival value, relevance to research or other preserved records, or other specified reason. (Advice may be sought from National Archives.)

A number of copies of the same document may be stored by recipients of that document, e.g. meeting papers. It is incumbent upon the person who has lead responsibility (i.e. Chair) for the retention of that record to retain the document for the requisite period and then to arrange for its disposal.

It is important that staff select the method of disposal in accordance with the type of record or data to be destroyed. Personal identifiable data must be confidentially destroyed by shredding or similar. Even many administrative records contain sensitive or confidential information. It is therefore vital that confidentiality is safeguarded at every stage and that the method used to destroy such records is fully effective and secures complete illegibility.

Disposal is the responsibility of the individual department or the record keeper.

Refer to SH IG 16 Records Retention, Archiving and Disposal Procedure

5.10 Information Asset Register & Data Protection Act compliance

Information Asset Owners and Administrators are responsible for maintaining an Information Asset Register, which documents all information assets (including records) for their operational area. This register will be subject to an annual review – managed by the Information Governance Manager.

5.11 NHS Code of Practice: Records Management – Records Inventory

The Trust will establish and maintain an inventory (which will link to the Information Asset Register) through which departments and services can register the records they maintain. The inventory of records will facilitate the classification of records into series, version control, the recording of the responsibility of individuals creating records, access control and the introduction of electronic document management. The register will aid identification and safeguarding key or vital records and support arrangements for business continuity. The register will be reviewed annually.

The Trust will maintain a register of records and records held by its predecessor organisations which have been transferred to National Archives.

Actions to be taken if policy is breached

Failure to comply with this policy may result in ineffective working and an inability to meet the requirements of the Data Protection Act and Freedom of Information. Where the policy is breached, this must be reported via the incident reporting process (i.e. via Ulysses Safeguard), and the Information Governance Manager and Caldicott Guardian informed, if required.
6. **Training Requirements**

All staff are required to complete annual Information Governance training via an online e-learning package and e-assessment to ensure competence and compliance.

E-learning applicable to specific roles, as identified by the service manager, will be completed by individuals via the Information Governance Training Tool or LEaD webpage.

Information Governance Training is mandatory for all staff every year.

See Appendix 1 – Training TNA.

7. **Monitoring Compliance**

This policy and its appendices provide compliance to the Information Governance Toolkit Standards, and compliance will be monitored as part of the annual submission, to comply with Monitor requirements.

8. **Policy Review**

This policy will be reviewed every three years (or sooner if new legislation, codes of practice of national standards are introduced).

9. **Associated Documents**

- SH IG 17 Information Governance Compliance and Framework
- SH IG 01 Records Keeping Policy and associated standards, procedures and guidance.
- SH IG 16 Records Retention Archiving and Disposal Procedure
- SH IG 18 Data Protection and Confidentiality Policy

10. **Supporting References**

- National Archives (Public Records) – [www.nationalarchives.gov.uk](http://www.nationalarchives.gov.uk)
- Records Management Code of Practice for Social Care 2016
### Appendix 1: Training Needs Analysis

If there are any training implications in your policy, please complete the form below and make an appointment with the LEaD department (Louise Hartland, Quality, Governance and Compliance Manager or Sharon Gomez, Essential Training Lead on 02380 874091) before the policy goes through the Trust policy approval process.

<table>
<thead>
<tr>
<th>Training Programme</th>
<th>Frequency</th>
<th>Course Length</th>
<th>Delivery Method</th>
<th>Facilitators</th>
<th>Recording Attendance</th>
<th>Strategic &amp; Operational Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Annual IG training for all staff</td>
<td>Annual</td>
<td>Approx. 1 hour</td>
<td>On-line e-learning and assessment</td>
<td>Content developed by Information Governance Manager</td>
<td>On staff’s personal LEAD account</td>
<td>Head of Information Assurance</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Directorate</th>
<th>Service</th>
<th>Target Audience</th>
</tr>
</thead>
<tbody>
<tr>
<td>MH/LD/TQ21</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Adult Mental Health</td>
<td>All staff</td>
</tr>
<tr>
<td></td>
<td>Specialised Services</td>
<td>All staff</td>
</tr>
<tr>
<td></td>
<td>Learning Disabilities</td>
<td>All staff</td>
</tr>
<tr>
<td></td>
<td>TQtwentyone</td>
<td>All staff</td>
</tr>
<tr>
<td>ISD’s</td>
<td>Older Persons Mental Health</td>
<td>All staff</td>
</tr>
<tr>
<td>ISD’s</td>
<td>Adults</td>
<td>All staff</td>
</tr>
<tr>
<td>ISD’s</td>
<td>Childrens Services</td>
<td>All staff</td>
</tr>
<tr>
<td>Corporate</td>
<td>All</td>
<td>All staff – including NEDs</td>
</tr>
</tbody>
</table>
Appendix 2: Equality Impact Assessment

The Equality Analysis is a written record that demonstrates that you have shown *due regard* to the need to *eliminate unlawful discrimination, advance equality of opportunity* and *foster good relations* with respect to the characteristics protected by the Equality Act 2010.

**Stage 1: Screening**

<table>
<thead>
<tr>
<th>Protected Characteristic</th>
<th>Positive impact</th>
<th>Negative impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Age</td>
<td>The policy covers all records in all formats (paper and electronic), both active and inactive held for use in the organisation, including administrative and clinical. The term <em>records lifecycle</em> describes the life of a record from its creation/receipt through its “active” use, then “inactive” retention (such as closed files which may still be referred to occasionally) and finally either confidential disposal or archival preservation. No adverse or potentially adverse impacts have been assessed.</td>
<td></td>
</tr>
<tr>
<td>Disability</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gender reassignment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Marriage &amp; civil partnership</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pregnancy &amp; maternity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Race</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Religion</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sex</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sexual orientation</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Stage 2: Full impact assessment**

<table>
<thead>
<tr>
<th>What is the impact?</th>
<th>Mitigating actions</th>
<th>Monitoring of actions</th>
</tr>
</thead>
</table>

Please describe the positive and any potential negative impact of the policy on service users or staff.

In the case of negative impact, please indicate any measures planned to mitigate against this by completing stage 2. Supporting Information can be found by following the link: [www.legislation.gov.uk/ukpga/2010/15/contents](http://www.legislation.gov.uk/ukpga/2010/15/contents)
Designing Record Keeping Systems

If the Trust/any of the services is designing new models of care they should use the DIRKS as identified in the NHS Code of Practice: Records Management 2016.

Design and Implementation of Record Keeping Systems (DIRKS)

The industry standard for the design and implementation of record keeping systems, as given in the ISO standard ISO15489-1:200131, is an eight stage process that can be summarised as:

1. Conduct preliminary investigation
2. Analyse business activity
3. Identify requirements for records
4. Assess existing systems
5. Identify strategies to satisfy requirement
6. Design records system
7. Implement records systems
8. Conduct post implementation review.

The below diagram indicates the relationship of the stages.

Further details can be sought from the Code of Practice for Records Management, the ISO standard and supplementary guidance. A privacy impact assessment must also be conducted where necessary. For more information please see the Records Management Code of Practice and the Information Commissioner’s Office (ICO) Privacy Impact Assessment Code of Practice.
Appendix 4 - Guidance on Specific Document Types:

Agendas, Minutes of Meetings and Associated Papers:

Only the Chair of the meeting is required to retain the meeting papers in accordance with the Trusts Retention Schedule. Other members who attend the meetings may keep their copies of papers at their own discretion.

Trust Board meeting minutes and papers are signed and kept as a hard copy.

Policies and Procedures:

The Trusts Clinical, Non-clinical, Human Resources, Finance and Information Governance policies are available from the website and word versions of them are maintained electronically in relevant folders managed by the Chair off the Policies and Procedures Committee. Their process for development, review and dissemination is documented separately.

Leaflets:

The Trusts leaflets will be maintained by the Communication Team, who will keep a register of all leaflets generated for use in the Trust.

Emails:

It is important that email messages are managed in order to comply with the Data Protection and Freedom of Information legislation. Staff need to be able to identify which emails (sent and received) are records of business activity and/or a formal record of a transaction (and therefore which need to be captured as records and save/located with other records relating to the same business activity) and which are ephemeral messages (which only need to be kept for as long as required and then deleted).

Mailboxes should not be used to long-term storage of emails messages. Personal mailboxes should be used for short-term reference only and when these emails are no longer required they should be saved on the relevant server or deleted.

Refer to the Trust Best Practice Guidance for Managing Emails.

Estates and Facilities Management (E&FM):

E&FM records are retained for at least the minimum periods in accordance with the Code of Practice as set down in the Retention Schedule, although in some instances for sound business reasons they may be kept for longer. The only exception to the Code of Practice relates to the retention of property documents and plans which requires Trusts to maintain these for the “lifetime of the organisation”. FM tend to keep these records “for the lifetime of the site and/or building to which they relate” and occasionally for a certain length of time afterwards.

Personal Files:

Recruitment and Employment:

On preparation of an offer of employment a Recruitment Personal File is established by the Recruitment Department which contains the application form and associated documents, the offer of employment and documents linked with the employment process.
Once the applicant has commenced employment and all the pre-employment checks are complete the Recruitment Personal file is forwarded to the recruiting manager, to be combined with the paperwork held at the place of work to form the Personal File for the employee. The files should be kept in a secure and lockable cabinet and access restricted to the appropriate personnel.

In the case that the employee transfers within the Trust the file should be forwarded to the new manager in a sealed envelope.

All Personal Files must be held securely by the manager responsible for the file at the time they have ownership of it.

Termination of Employment:

On termination of employment the manager should complete the termination form for the employee, keep one copy in the Personal File and forward the remaining copies to HR by the date that employment ceases. HR will terminate the employment on ESR ensuring that all outstanding payments are made.

Retention of Personal Records:

The file will be kept for the appropriate period (for 6 years) and will be destroyed at the end of this period. The employment summary document will be retained in the Trust for the appropriate period (70th birthday of the employee).

Finance Records:

The Trusts Finance Directorate will have responsibility for retaining all prime finance documents on behalf of the organisation, with the exception of any financial reports, (including the Trusts annual accounts), which are received by the Trust Board, where responsibility will lie with the Trust Secretary. Therefore whilst operational managers may retain copies of budget statements for their own particular area, a master copy in compliance with the retention policy will be retained by the finance department. Any copy retained by the manager must be disposed of in line with the retention policy.

Where local arrangements are in place for original receipts in support of petty cash reimbursement or cash receipts which require these records to be retained locally rather than within the finance department, then these must also be retained as per the policy by the department, rather than by Finance.