Hertfordshire Community NHS Trust is committed to being an organisation within which diversity, equality and human rights are valued. We will not discriminate either directly or indirectly and will not tolerate harassment or victimisation in relation to gender, marital status (including civil partnership), gender reassignment, disability, race, age, sexual orientation, religion or belief, trade union membership, status as a fixed-term or part-time worker, socio-economic status and pregnancy or maternity.

(i) This document is available electronically, in a larger font, or alternative format on request.
## Document History and Version Control

<table>
<thead>
<tr>
<th>(A) Document Progress and Circulation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Preliminary Draft:</strong> v.1</td>
</tr>
<tr>
<td><strong>Consultation Drafts:</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Edition 3</strong></td>
</tr>
<tr>
<td><strong>Approval Draft</strong> v 2</td>
</tr>
<tr>
<td>v 3</td>
</tr>
<tr>
<td><strong>Approved Document Circulation List:</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Date Circulated:</strong></td>
</tr>
</tbody>
</table>
(B ) Historical Editions

<table>
<thead>
<tr>
<th>Edition and Date</th>
<th>Reason for Archiving</th>
<th>Date of Archiving (including archive location)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1&lt;sup&gt;st&lt;/sup&gt; Edition v1 (March 2011)</td>
<td>Superseded by 2&lt;sup&gt;nd&lt;/sup&gt; Edition</td>
<td>May 2011 N:HCT/ Shared Secure/Archived Policies</td>
</tr>
</tbody>
</table>

(C) Implementation Plan:

<table>
<thead>
<tr>
<th>Action:</th>
<th>By Who:</th>
<th>When:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dissemination via electronic staff Noticeboard</td>
<td>Policy Administrator</td>
<td>Within 2 weeks of approval</td>
</tr>
<tr>
<td>Cascade to all staff</td>
<td>Heads of Service and Locality Managers through staff briefings and meetings</td>
<td>Within 1 month of Approval</td>
</tr>
<tr>
<td>Monitoring of adherence at local level through line management process</td>
<td>Heads of Service and Locality Managers</td>
<td>Annually/or as per monitoring arrangements</td>
</tr>
<tr>
<td>Provide specific training relevant to this policy:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Training content and target individuals / groups to be identified.</td>
<td>Lead Officer to liaise with Learning &amp; Development Team</td>
<td>Within 2 weeks of approval</td>
</tr>
<tr>
<td>Learning and Development Team to co-ordinate training provision.</td>
<td>Learning and Development Team</td>
<td>Within 1 month of approval</td>
</tr>
<tr>
<td>Training delivered</td>
<td></td>
<td>Within 4 months of approval</td>
</tr>
<tr>
<td>Ongoing individual / group training needs to</td>
<td></td>
<td>Continuous</td>
</tr>
</tbody>
</table>

Page 3 of 75
be identified as part of appraisal and training needs analysis (TNA) process.

(D) Procedural Document Acknowledgements

(1) CP04 Guidelines for the Development and approval of Documents across Provider Services (undated)


(E) Amendment Log

<table>
<thead>
<tr>
<th>Edition</th>
<th>Version</th>
<th>Type of Change</th>
<th>Date</th>
<th>Summary of Changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>3rd</td>
<td>2</td>
<td>Six month review</td>
<td>May 2012</td>
<td>Re-write following NHSLA comments</td>
</tr>
<tr>
<td>3rd</td>
<td>3</td>
<td>One year review</td>
<td>June 2013</td>
<td>Amendment to Appendix 4 archiving and the inclusion of standard operating procedures for archiving</td>
</tr>
</tbody>
</table>
Contents

1.0 Policy Statement .................................................................6
2.0 Purpose and Scope of Policy / Procedure..................................7
3.0 Application.............................................................................7
4.0 Exceptions.............................................................................8
5.0 Definition of Terms................................................................8
6.0 List of Abbreviations............................................................9
7.0 Accountability and Responsibilities (Duties)..............................10
8.0 The Use of Records ................................................................15
9.0 Confidentiality/ Caldicott Principles .........................................15
10.0 Record Quality .....................................................................16
11.0 Record Management............................................................24
12.0 Access and Recovery............................................................32
13.0 Education and Training............................................................36
14.0 Implementation and Monitoring of Compliance .........................37
15.0 Reviewing, Updating and Archiving........................................37
16.0 Interpretation .......................................................................38
17.0 References and Associated Documents .......................................38
18.0 Document Checklist...............................................................40
19.0 Equality Impact Statement and Assessment .................................41

Appendix 1 Guidance on the Maintenance of Personnel Files .............42
Appendix 2 Confidentiality Statement and Agreement ..........................53
Appendix 3 Core Content in clinical records.................................55
Appendix 4 Archiving Procedure and Process for Retrieval of Records ....57
Appendix 5 Internal Confidential Courier Service (“Red bag” Scheme) .....61
Appendix 6 Access to Health Records Checklist ..................................65
Appendix 7 Mandatory Training Framework .....................................66
Schedule 1 Committee Structure/Reporting Flow-Chart (September 2012) For
This Policy ................................................................................67
Schedule 2 Document for Compliance Monitoring ..........................68
Schedule 3 Document Checklist.....................................................72
Schedule 4 Equality Impact Assessment ........................................75
1.0 Policy Statement

1.1 Hertfordshire Community NHS Trust (“The Trust”) is committed to:

(i) complying with statutory and regulatory requirements as prescribed by the Department of Health guidelines issued by the Caldicott Committee 1997 (reviewed 2013) and governmental and legal requirements:

- Audit Commission setting the record straight 2002
- Caldicott Manual 2010
- Information Governance Review
- Confidentiality, NHS Code of Practice, 2006
- CQC Essential Standards of Quality and Safety Outcome 21 Regulation 20
- Data Protection Act 1998
- European Data Protection Directives 95/46/EC
- ISO 27000 - An Introduction to ISO 27001
- Freedom of Information Act 2000
- Information Governance Toolkit
  https://nww.igt.connectingforhealth.nhs.uk/
- NHSLA Standards 2012 - 2013.pdf
- Records management: NHS Code of Practice parts 1 and 2 (270422/1 and /2)

(ii) the potential risk for non-compliance with managing records is the risk of litigation and the organisation not meeting the requirements of external reviews such as NHSLA Standards, CQC Essential Standards of Quality and Safety standards and the Information Governance Toolkit.

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

Nb: Staff are currently following these policies from the predecessor organisation, NHS Hertfordshire (the Primary Care Trust).

(i) Freedom of Information IG003 FOI Policy Jan 13.doc
(ii) Code of Conduct for Staff in Respect of Patient and Staff Confidentiality IG 003 Code of Conduct on Confidentiality Jan 2013.pdf
2.0 Purpose and Scope of Policy / Procedure

2.1 This policy is based on The Records Management: NHS Code of Practice which has been published by the Department of Health 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. It is based on current legal requirements such as the Data Protection Act 1998 and on professional best practice. Records Management is the process used by the organisation to manage all aspects of records whether internally or externally generated and in any format or media type, from their creation, all the way through their lifecycle to their eventual disposal.

2.2 Effective implementation aims to achieve good practice in record keeping across the Trust in order to provide accurate contemporaneous record-keeping in all formats regardless of how they are held; and the ongoing audit of record-keeping standards which should have a specific focus on each of the minimum requirements within this process, as identified in the NHSLA Risk Management Standards and to ensure that legal requirements for record keeping practice are met across the Trust.

2.3 The policy sets out the main requirements for the management of all clinical and non-clinical records within Hertfordshire Community NHS Trust (The Trust) to ensure that they are effectively and lawfully managed. These include:

(i) all administrative records (e.g. personnel, financial and accounting records, service level agreements, notes associated with complaints); and
(ii) all service user health records (including their medical case notes, nursing care plans, visual or audio recordings, registers etc.)

2.4 The term ‘records’ applies to electronic and paper records that provide evidence of actions and decisions made by the organisation and therefore they are its corporate memory. The electronic record is intended to be the ‘primary record’, to replace paper files in the day-to-day management of service user information and corporate decision making. It is the main source of information sharing in the clinical and managerial environment.

3.0 Application
3.1 The policy and procedures in this document apply to all clinical and non-clinical records managed by the Trust and shall be adhered to by all clinical and non-clinical Trust staff (including Bank, Agency, Interim staff and staff on fixed term contracts). For personnel files please refer to Appendix 1. Managers of services are responsible for ensuring compliance within their teams, in consultation with, and seeking support from the Assistant Director of Performance and Information, the Compliance Manager and/or the Caldicott Guardian as appropriate and necessary. The committee structure chart (Sept 2012).doc outlines the strategic committees responsible for overall responsibility for the Records Management and Information Lifecycle Policy and Procedure.

4.0 Exceptions

4.1 This policy does not apply to Subject Access Requests made under the Data Protection Act 1998, for which the following applies:

   (i) Policy on Subject Access Requests and the Data Protection Act Data Protection Act 1998.mht

4.2 This policy does not apply to the Freedom of Information requests for which the following applies:

   (i) Freedom of Information Policy, IG003 FOI Policy Jan 13.doc.

5.0 Definition of Terms

5.1 Records Management

5.1.1 Record 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:

- record creation
- record keeping
- record maintenance (including tracking of record movements)
- access and disclosure
- closure and transfer
- appraisal
• archiving; and
• disposal

5.2 Records Life Cycle

5.2.1 Records Life Cycle describes the life of the 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.

5.3 Records

5.3.1 Records are defined as ‘recorded information’, in any form, 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.

5.4 Information

5.4.1 Information is a corporate asset. The Trust's records are important sources of administrative, evidential and historical information. They are vital to the Trust to support its current and future operations (including meeting the requirements of the Freedom of Information legislation) for the purpose of accountability and for an awareness and understanding of its history and procedures. Service user information incorporates patient records.

6.0 List of Abbreviations

6.1 The following are abbreviations used throughout this document:

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CD / CDs</td>
<td>Controlled Drug/s</td>
</tr>
<tr>
<td>CQC</td>
<td>Care Quality Commission</td>
</tr>
<tr>
<td>DH</td>
<td>Department of Health</td>
</tr>
<tr>
<td>DPA</td>
<td>Data Protection Act</td>
</tr>
<tr>
<td>EPR</td>
<td>Electronic Service user Record (former Electronic Patient Record)</td>
</tr>
<tr>
<td>FOI</td>
<td>Freedom of Information</td>
</tr>
<tr>
<td>HCT</td>
<td>Hertfordshire Community NHS Trust (&quot;The Trust&quot;)</td>
</tr>
<tr>
<td>IG</td>
<td>Information Governance</td>
</tr>
</tbody>
</table>
7.0 Accountability and Responsibilities (Duties)

7.1 Committee Lines of Reporting and Assurance

7.1.1 The Committee Lines of reporting and assurance through to the Trust Board in respect of this document is as identified in committee structure chart (Sept 2012).doc

7.2 Trust Board

7.2.1 The Board has responsibility for:

(i) directly or indirectly through the Designated Committee (see below), receiving assurances (positive or negative) that this document is effectively implemented, monitored and complied with.

7.3 Designated Committee

7.3.1 The “Designated Committee” for this Records Management and Information Lifecycle Policy and Procedure is the Information Governance Group. The Designated Committee is responsible for:

(i) approving this document
(ii) receiving reports from the Lead Officer on the compliance for the implementation of this Document (including any education and training compliance) as arising from compliance monitoring arrangements prescribed in Schedule 2

7.4 Executive Team

7.4.1 The Executive Team has collective responsibility for ensuring that:

(i) effective systems, processes and resources are in place for the implementation of, and compliance with, this policy.

7.4.2 The Committee Line of Reporting through to the Trust Board in respect of this Policy / Procedure is as set out in Schedule 1.
7.5 Other Groups

7.5.1 The Information Governance Group chaired by the Senior Information Risk Owner (SIRO) is a sub group of the Trust Executive which is led by the Chief Executive and reports to the Trust Board. The SIRO with support from the Director of Performance and Information and the Caldicott Guardian and Senior Managers of the Trust are accountable for records management within the organisation and have a duty to make arrangements for the safekeeping of the records. Additionally the Caldicott Guardian is responsible for approving and monitoring national and local guidelines and protocols on the handling, sharing and management of confidential service user information and organisational sensitive data ensuring that appropriate controls are in place. Anyone who records, handles, stores or otherwise comes across service user information has a common law duty of confidence to people accessing NHS services. This duty continues even after the death of an individual.

7.5.2 The Information Governance reference group is a sub group of the Designated Committee, the Information Governance Group. The overall objective of this group is to ensure the development, implementation and review the compliance of the Trust's policies on Information Governance, including the management of all records, whether clinical or corporate.

7.5.3 The Clinical Effectiveness sub committee (CES) is a sub group of the Health Care Governance Group. The Clinical Record Keeping audit results are presented at CES and the Information Governance Group.

7.6 Chief Executive

7.6.1 The Chief Executive, as the Accountable Officer for the Trust, has overall accountability and responsibility for ensuring that:

(i) the effective operational implementation of this document and
(ii) the Executive Team complies with its responsibilities under s.7.4 above and
(iii) that the named Lead Executive Director fulfils their responsibilities under this document.

7.7 Lead Director

7.7.1 The Lead Director is the Director of Finance and is responsible for:

(i) affirming the Lead Officer and directing them during the course of the development of this policy
(ii) signing off this policy as approved for circulation and implementation following approval by the Designated Committee (or its delegate)
(iii) overall supervision of the effective development and implementation of this policy and
(iv) reporting to the Chief Executive and Executive Team any significant issues arising from the implementation of this policy, including evidence of non-compliance arising from the monitoring process, so that remedial action can be undertaken
(v) arbitrating on any questions of interpretation arising from this policy.

7.8 Lead Officer

7.8.1 The Lead Officer is the Compliance Manager and is responsible for:

(i) preparing, drafting, consulting on, and steering this policy through to the approval, signing-off and distribution stage
(ii) following the implementation plan, including ensuring that this policy as approved is circulated and publicised. This shall include as a minimum submitting the policy for posting on the staff intranet
(iii) monitoring the compliance of this policy in accordance with Schedule 2 Document for Compliance Monitoring
(iv) ensuring that this policy is reviewed in accordance with the prescribed timescale
(v) reporting evidence of non-compliance to the Lead Director (for action) and to the Designated Committee (for assurance purposes)
(vi) submitting this policy to the Policy Administrator for archiving when it is no longer valid.

7.9 General Managers/Assistant Directors

7.9.1 General Managers/Assistant Directors and through their Line Managers are responsible for ensuring that:

(i) this policy is available and accessible to their staff
(ii) their staff are aware of this policy and understand their responsibilities
(iii) their staff are trained in accordance with this policy and as identified under a Training Needs Analysis
(iv) their staff comply with this policy and that any evidence of non-compliance (individually or
collectively) is reported to the Lead Officer and Lead Director

(vi) taking such action to ensure compliance
Action may include:
- access to training
- use of personal development/appraisal process
- providing clear instructions and / or briefings to individuals or groups
- in extreme cases, use of performance management/ disciplinary procedures

(vi) their staff co-operate with the Lead Officer in the exercise of their compliance monitoring function and that any evidence of lack of compliance for whatever reason is brought to the attention of the Lead Officer.

7.9.2 General Managers/Assistant Directors have specific duties as Information Asset Owners. Their role is to understand and address risks to the Information Assets that they ‘own’ and to provide assurance to the SIRO on the security and use of these assets.

7.10 Line Managers

7.10.1 As directed, Line Managers will support their General Managers/Assistant Director in the carrying out of their responsibilities under s. 7.9 above.

7.10.2 Managers of services have responsibility to ensure compliance within their areas, making sure records management issues are discussed in supervision and key performance targets around record keeping including training are met. Managers need to be fully conversant with the electronic records and computer system and supplementary reporting procedures that are used in their service area.

7.10.3 Managers are responsible for maintaining the security of clinical records in general and for ensuring access permissions for the electronic service user record (EPR) are appropriate and upheld. This also applies to other information systems such as Datix, for incidents, complaints and the patient advice and liaison service.

7.11 All Staff

7.11.1 All staff have a responsibility to:
(i) understand this policy and their responsibilities outlined in this section
(ii) comply with the provisions of this policy
(iii) attend or undertake any training in respect of this policy as identified by their Line manager
(iv) raise with their Line Manager any issues or concerns they may have in respect of this policy, including their understanding or ability to comply with their responsibilities
(v) report in confidence known breaches of this policy by others to their Line Manager where such breaches have presented or may present a risk of, or actual, significant harm or loss to patients, staff, the public or the organisation as a whole
(vi) report honestly and openly instances to their Line Manager where they are aware that they have individually been in breach of their responsibilities, and where such breach has presented or may present a risk of, or actual, significant harm or loss to patients, staff, the public or the organisation as a whole.

7.11.2 NB: Staff are advised to note that:

(i) the Trust operates a culture of “Fair Blame” whereby other than in exceptional circumstances, disciplinary processes are usually a last, rather than a first resort
(ii) there may be occasions where breach of a Procedural Document may be a disciplinary matter.

7.11.3 Additional responsibilities:

(i) staff need to keep up to date and adhere to, relevant legislation and national and local policy relating to information and record keeping
(ii) keep up to date on best practice for health care records and communication practice standards
(iii) be proficient in the system they use to record and communicate health and social care information
(iv) meet the standards of their professional organisation.

7.12 Caldicott Guardian

7.12.1 Additional to the strategic role in regard to representing and championing information governance, the Caldicott Guardian has a fundamental role around confidentiality; justifying and
testing that the organisation and partner organisations satisfy the highest practical standards for handling patient identifiable information, ensuring patient identifiable information is shared only for justified purposes, and that only the minimum information is shared and stored and collected.

(i) last, rather than a first resort.
(ii) there may be occasions where breach of a Procedural Document may be a disciplinary matter.

8.0 The Use of Records

8.1 Records are a valuable resource and must be managed and available to members of staff as required and appropriate in order to:

(i) support the care and continuity of care of service users, whilst maintaining their confidentiality.
(ii) support clinical and managerial compliance through multi-disciplinary working within the Trust and with partner agencies.
(iii) support day-to-day business that underpins the care and work of service users.
(iv) support evidence based clinical practice.
(v) assist in providing evidence for internal and external reviews and other audits.
(vi) support sound administrative and managerial decision making.
(vii) meet legal requirements including requests from service users under access to health records legislation.
(viii) provide and/or publish organisational information in line with statutory requirements relating to freedom of information and accountability / transparency in use of public resources.
(ix) enable and empower the Trust to support improvements through audit and research and archival functions by taking account of the historical importance of material and the needs of future research.
(x) support the investigation of complaints, claims and incidents.

8.2 Where NHS services are being planned or provided with other agencies, the procedures and guidance set out in this document should be followed.

9.0 Confidentiality/ Caldicott Principles

9.1 Service users and staff have the right to object to the use and disclosure of confidential information. Therefore they need to be informed of the reasons why information is documented and why it is to be shared with other professionals. Staff should ensure that the service user or member of staff is given an informed choice. Patients should be
given the leaflet ‘Protecting and using of personal information – your rights’, their understanding should be verified and the relevant professional should reconcile their concerns and honour their objections. Certain Acts of Parliament require disclosure, and the courts may also order disclosure.

9.2 The amount disclosed should be proportionate to actual need. The service user or member of staff needs to be informed of what has been or will be disclosed. Refer to Confidentiality NHS Code of Practice

9.3 If the service user is competent to consent then the health professional should ensure that the information provided is in a suitable form or language. If the service user is unable to give consent due to mental or physical condition then health professionals must take into account the service user’s values and wishes and act in their best interests and any previously expressed wishes or Advanced Decision (Mental Capacity Act, 2005). Please refer to Hertfordshire Mental Capacity Hertfordshire Policy on Mental Capacity for further information.

9.4 Records must be kept secure and should be stored in an appropriate filing cabinet, office or designated records store so they are available and accessible to those who need them. For further information please refer to the Code of Conduct on Confidentiality

9.5 In addition, all members of staff employed by the Trust, whether on permanent or short-term contracts, are expected to abide by the Trust confidentiality and data protection policies. Contractors and consultants employed by the Trust should sign the Confidentiality Statement located in APPENDIX 2 Confidentiality Statement and Agreement. All health professionals are responsible for their own code of conduct as indicated by their professional body and body of registration.

9.6 There are five phases of the Information lifecycle: Creation, Retention, Maintenance, Use and Disposal.

10.0 Record Quality

10.1 Creating records. Non-Clinical and Clinical Records

10.1.1 Electronic files should be stored in appropriate folders and individual documents should be identifiable, so that the most recent documents can be quickly located. Information retained must be in line with the Data Protection Act 1998, Confidentiality NHS Code of Practice and ISO 27001. It is the responsibility of all staff to ensure security and confidentiality of records in their possession and to be aware of ways in which these responsibilities may be contravened.
10.1.2 The **Information Security Policy** provides detailed instructions relating to the security of the Trust information systems and must be read in conjunction with these guidelines.

10.2 Clinical records (including those held in service user homes and care homes) are the property of the Trust on behalf of the Secretary of State for Health. They are not the property of the patient, relative, carer or staff member. If there is agreement in service specifications that the Trust’s staff will record care given by them in the records of another Trust, the records remain the property of that Trust.

10.3 Naming Files

10.3.1 Naming conventions are standard rules to be used for naming both electronic files and folders. Using the Trust naming convention will help to identify documents more quickly. The following rules must be followed when entering documents onto the computer either for clinical or non-clinical use.

10.3.2 **Specific** information should be recorded when naming a document e.g. the content of the document.

10.3.3 **Logical** information should also be captured e.g. the name of the person who created the document and the date the document was created (not the date it was entered onto records).

10.3.4 Each file must have:

- (i) a **unique name** and number e.g. service user’s NHS number and patient name to each document
- (ii) a meaningful name which closely reflects and records content
- (iii) express elements of the name in a structured and predictable order
- (iv) locate the most specific information at the beginning of the name and the most logical at the end.

10.3.5 All clinical documents should have ‘please return this document’ to the relevant service’s address on the front.

10.3.6 Clinical records should be marked confidential and given a volume number (if more than one volume).

10.3.7 Non-clinical records that need to be security marked should have: -
(i) **Version Control:** Each document must contain the name and version control in the header and page number x of y in the footer.

(ii) **Watermarks:** All draft documents must always contain a watermark stating the document is DRAFT. This will avoid confusion for any potential reader and prevent staff from believing the document may be an approved document. This will be removed once it has been approved.

(iii) **Distribution Lists:** The distribution or circulation list of certain documents (e.g. agendas, consultation drafts etc) must be clearly marked on all copies to avoid unnecessary duplication and to facilitate the recipients forwarding the document onto others who may also need to see it.

10.4. Record keeping in clinical notes. **Individual Responsibility**

10.4.1 High quality clinical and corporate record keeping and collection of relevant information is one of the main components of Clinical and Corporate Governance and improves and supports Service User Safety.

10.4.2 Each member of staff is individually accountable for maintaining the clinical records of service users on their caseloads. All clinicians providing treatment and care for service users are responsible for inputting their own information into the Electronic Service user Record (EPR) and to update their contacts and clinical details.

10.4.3 Confidentiality, NHS Code of Practice and Health Professional bodies’ state that individuals should ensure that all health records (electronic/paper) and corporate records:

   (i) are clear, accurate, legible and contemporaneous (recorded within 48 hours and not more than 5 days after the event) and where not electronic written in black ink.

   (ii) provide a record of all the health and social care interventions undertaken by staff, including those seconded from other agencies and the service user and carer’s response.

   (iii) provide information which will facilitate communication between staff and service user to enable continuity of care.

   (iv) provide evidence of negotiated care and understanding of the actions agreed between service user or a relative/carer and the health or social care worker.
(v) provide documentation of information given to service users.

(vi) do not include personal views about the service user’s behaviour or temperament unless these have a potential bearing on treatment. Meaningless phrases, irrelevant speculation or offensive comments about the service user, their relatives, or other individuals must not be used. (Please refer to the Information Commissioner’s *Data Protection Good Practice Note – How does the Data Protection Act apply to professional opinions?* (2008), Available from: [http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/how_does_the_data_protection_act_apply_to_professional_opinions.pdf](http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/how_does_the_data_protection_act_apply_to_professional_opinions.pdf)

(vii) should clearly identify the date, time, which person created the document, during which operational process and link it to the referral.

(viii) hold information that is entered consecutively.

(ix) where amendments are made, these should be scored through with a single line and signed and dated and timed.

(x) the record reliably represents the information that was actually used in or created by the operational process and its integrity and authenticity can be demonstrated.

(xi) the record can be maintained through time. There is no unnecessary duplication between the paper and electronic record collections.

(xii) provide information that will support clinical compliance, audit and Health or Social Care research.

(xiii) health professionals should ensure the security and confidentiality of the records in their care.

(xiv) health professionals who document their care in service users hand held records should ensure that a record of their visit is entered into a centrally held electronic record. Where there are concerns regarding the security of the record in the service user’s home, the health professional is advised to document the care given in a separate file held by the health professional.

(xv) complaint correspondence should not be included in clinical notes as this could be seen to prejudice a patient’s future case.

(xvi) such correspondence is held in a centrally held complaint file. Refer to the [Complaints Policy](#).
10.4.5 Health professionals are accountable for the entries made by support workers, students or other people under their supervision in records of service users under their care.

10.5 Core Content in clinical records.

10.5.1 Personal details contained in the record must be checked for accuracy and updated accordingly each time the individual sees the service user. Any discrepancies should be confirmed by the member of staff and any amended in the EPR/health care record.

- Name
- Address (incl. postcode)
- Contact telephone
- GP details
- Next of kin or agreed contact as identified by the service user

10.5.2 Clinical records must clearly identify the service user to whom they refer and include: assessment, care given, rationale, discussions, consent/ declining of consent and clinical decision making APPENDIX 3 Core Content in clinical records.

10.5.3 Records must be recorded in English, and must be clear and legible. Records must be created in terms, which the service user and other professionals will be able to understand. Jargon should not be used as the record should be written in terms the service user is able to understand. Records should be kept in chronological order.

(i) Alterations to a clinical note are not acceptable. The original entry must be marked invalid and left in the record. A new note must be entered with a reason for the cancellation of the original entry. Please note: EPR clinical notes can be edited after being saved in the system. However, once the note is confirmed it can no longer be edited and must be marked invalid as above. Clinical notes must be entered saved and confirmed immediately they are completed.

(ii) Additions must be dated timed and signed. User login id and password creates the electronic record signature.

(iii) All entries must be accurate as to date (day, month and year) and time (24 hour clock). The date and time of the event must be recorded and the time the record was written clearly noted.

(iv) Clinical notes must be entered as soon as possible following a contact; the minimum standard is within
48 hours and no longer than 5 days. Where this is not possible and there is a significant delay in recording the information, an explanation should be added at the start of the note, giving the reason for the delay and the date and source of any original notes taken.

(v) If an entry is to be highlighted, for ease of identification or to provide instruction, this should be done by using CAPITAL LETTERS and recording the name or instruction, e.g. ‘NOT FOR DISCLOSURE’ in the title or summary field.

(vi) All information should be clear and unambiguous, factual, consistent and accurate. Relevant, non-factual entries e.g. conclusions or opinions may be recorded and should be indicated as such.

(vii) There must be no discrepancies between the information in the electronic service user record and the secondary paper. An entry to direct the reader to the EPR must be made in the paper file, which should be referenced using the ‘records locator’ on the system.

(viii) The name of any patient information document, the edition number, version and the date given to the patient should be recorded in the patient record. External information that is given to patients should be referenced and dated i.e. Diabetes UK website details and the date details given.

(ix) A copy of the ‘front page’ from the EPR should be printed and stored in the secondary paper file. This must be dated at the time of insertion into the file and updated with any changes as appropriate or at the start of any subsequent spell of care.

(x) Documents which should not be disclosed should be marked "review before access".


10.6 Letters and signatures

10.6.1 Any communication relating to patient treatment/care must have a written or a scanned clinician signature attached and be on Trust headed paper. All patient letters should be checked by a clinician for accuracy prior to being sent out. It is
preferable that the letter is checked and agreed by the clinician who has written the letter. However, if the clinician who drafted the letter is unavailable the letter can be checked for accuracy by another clinician who would then need to sign their own name (put a pp before the signature). If there has been agreement by a clinician that the letter is pp’d by an administrator there needs to be a clear audit trail to show that the clinician has checked and agreed the contents of the letter before it is sent out. Remember to check not just clinical content but the accuracy of names, addresses and personal details. Refer to the Standard Operating Procedure for the Processing of Correspondence containing person identifiable information. [SOP Processing and handling correspondence which includes PII.doc](#)

10.6.2 A full distribution list of all those that it is sent to should be included. It should also be copied to the service user and to others with the service users consent

10.6.3 Standard (e.g. appointment letters) do not need to have a clinician’s signature. But do need to indicate their source e.g. sent but not signed by service administrator.

10.6.4 Ensure that there is a return address on the outside of the envelope if the letter is to be posted.

10.7 Entries by non-Trust employees

10.7.1 The EPR system is only available to Trust staff for direct entries. From time to time it may be necessary to provide read only access to service user records for legal and audit purposes. And this will be done using information governance and Caldicott principles.

10.7.2 Entries to the paper health record by other agencies should be made on a separate sheet, signed and dated and attached in the paper record or scanned onto the EPR.

10.8 Service user held records

10.8.1 Service user held records allow the service user to be closely involved with their care and encourages partnership between the service user and the health practitioner. The following need to be taken into consideration:

(i) the service user needs to give consent / decline consent on how the clinical record is shared within the multidisciplinary team.

(ii) they should only be used where appropriate and with the service users consent.
(iii) the service user should be informed of the purpose and importance of the record and their responsibility for keeping it secure and safe.

(iv) they must be reminded that these records are confidential to themselves and the health or social care team.

(v) the record should not contain information that is likely to cause harm or distress to the service user and must be in terms and language that they can understand.

10.8.2 Such records are not the property of the service user; the records must be returned to the Trust for storage at the close of an episode of care. Service users, relatives and carers must be made aware of their responsibilities in relation to the care of the Trust records whilst in their possession. The exception to this is the parent child health record that is given to the child from birth; this is a health record for that individual. If the service user record is multi-agency, then it is the health professional’s responsibility to ensure that the episode of care is documented in a centrally held record (electronic or paper format).

10.8.3 Service user held records must be returned on request to enable an investigation into a Serious Incident, complaint or similar to be conducted. If service user held records are not returned, a staged process is to be followed:

- Stage 1 (Local resolution): the lead practitioner for the service user will contact the family and/or service user to request the records and reinforce the responsibilities that the service user, relatives and carers have with regard to Trust records in their possession
- Stage 2: a formal approach is made by the tier 4 locality manager to request records
- Stage 3: a formal request is made by the Deputy Director of Operations for the return of the Trust record
- Stage 4: a formal request is made by a Director for the return of the Trust record. Legal advice will be sought at stage 4.

10.8.4 As part of the service user’s participation in the care process, they may wish to write about their experiences. These notes should be written on separate sheets and attached to the care record. The notes should be signed and dated by the service user. The health professional needs to acknowledge their notes and deal with any issues highlighted and document their actions.

10.9 Controlled Drug Registers
10.9.1 Service held records are held in accordance with the Controlled Drugs Department of Health. Records for schedule 2 CDs must be kept in a controlled drug register. All healthcare professionals who hold CDs must keep their own controlled drug register and are responsible for the accuracy and that it is up to date. Refer to Medicines and Medicines Safety Policy.

10.9.2 Under the Health and Social Care Act 2008, the police have powers to enter any premises where controlled drugs are used and to inspect any records relevant to such use and take copies or take possession of records for as long as the person exercising the power considers necessary. The Care Quality Commission also has the power of entry to view clinical records where appropriate.

10.10 Audit

10.10.1 Audit is part of the risk management process and there will be annual audits of the quality of record keeping standards to ensure an ongoing programme of improvement. The audit will be multi-professional and include completeness of data and quality of content, as required by NHSLA standards for Trusts. The audit of clinical records is carried out by the services, co-ordinated and supported by the audit team. The outcomes are reported to the HealthCare Governance Committee via the Clinical Effectiveness sub-committee. The audit templates are reviewed annually and are available from the audit team. The results are shared with the Information Governance Group.

10.10.2 The audit of corporate records are carried out by the Information Governance group as part of its work plan.

10.10.3 This policy should be read in conjunction with the Clinical Audit Policy.

11.0 Record Management

11.1 Storage/ Filing

11.1.1 The storage of all records must be in accordance with Health and Safety requirements and legislation.

(i) A secondary paper file can be used to store specific documents i.e. photographic images of patients. There must be cross references between both electronic and paper records. All other documentation within the Trust must be reviewed annually and stored in accordance to the
Department of Health’s archiving policy, which can be found at http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4131747

(ii) Contents within manual records should be stored chronologically, the most recent part of the records accessible first. This applies to each section if so split.

(iii) All images of patients i.e. film recordings should be stored electronically on a secure drive or in the paper record.

(iv) Storage arrangements must allow for retrieval with speed of access dependant on the urgency of requirement of access to the information. Refer to the Trusts Archiving Procedure and Process for Retrieval of Records APPENDIX 4 Archiving Procedure and Process for Retrieval of Records.

(v) Information printed from the EPR should be shredded once it is no longer required – after updating the EPR with any changes. Hand written notes and messages can also be shredded once the information has been transferred to the EPR.

(vi) The EPR system has a robust and reliable back-up system that enables retrieval of the most up-to-date backed up files in the cases of an accident or disaster preventing access to the main record storage.

(vii) For local sites the EPR should be able to produce printed versions of the relevant parts of the record in the case of local network failure.

(viii) Staff should not take service user records home. Where this cannot be avoided a procedure for safeguarding the information should be locally agreed.

(ix) Manual records should not be left where unauthorised people could accidentally see the contents. Keep the file closed or cover the information.

11.2 Scanning

11.2.1 Information must be typed directly into the appropriate documents within the EPR. Handwritten then scanned attachments are to be avoided. Where additional documents / tools are used and inclusion in the EPR is considered relevant, they may be scanned and attached, or if very large, a brief summary should be entered into the clinical notes section, with a reference to where the original is stored i.e. the secondary paper file.
11.2.2 All scanned documents must be dated and titled appropriately to enable easy identification and retrieval. The date should reflect the date of the correspondence/activity/incident, not the date it is being attached to the record.

11.3 Tracing Records

11.3.1 The Trust is responsible for ensuring tracer systems are implemented for all types of record management to enable the whereabouts of a specific file to be known at all times. Examples would include Critical Incident Review Files, Complaints Files, and Personnel Files. Refer to Appendix 1 Guidance on the Maintenance of Personnel File1.doc.

The minimum data which needs to be recorded includes: the name of the file; date the file was dispatched, destination, name of recipients and name of person releasing the file. A return receipt should always be requested and made clear to whom the records should be returned and by when. A chase and tracking system must be operated to ensure the file is safely returned to the relevant filing system and that absent records are chased regularly.

11.3.2 Example of a tracer card for patient paper records:

<table>
<thead>
<tr>
<th>TRACER</th>
<th>File Name:</th>
<th>Location:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Date Sent/Removed</td>
<td>NHS Number</td>
<td>Name of person releasing the file</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
11.3.3 Example of a tracer card for non patient paper records

<table>
<thead>
<tr>
<th>Date</th>
<th>Name of person removing</th>
<th>Name / Name of Document</th>
<th>Location and Person Sent To</th>
<th>Date / Method Confirmed receipt</th>
<th>Date Returned</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

11.3.4 It is important that a tracer system is maintained for each stage in the file’s journey, for example, when Person A sends a file to Person B, Person A will maintain a record of the file’s date of dispatch, destination and will request an acknowledgement of receipt. If Person B then passes the file on to Person C, it is the responsibility of Person B to maintain their own record of the file’s transfer to Person C and its subsequent location.

11.3.5 If patient paper records are missing for a clinic or an appointment, the clinician will assess the risk to the patient of the appointment being delayed. The assessment or treatment may be able to proceed if sufficient details are available either electronically or by telephone contact with the referrer and if the patient is in agreement.

11.3.6 When a patient record is missing every effort should be made to trace it before the assessment or treatment is due. If it cannot be found before the day the assessment or treatment is due then a duplicate record should be created and utilised. In addition, the process of investigation as to why the patient record was missing should commence within 48 hours of the record being found to be missing. Duplicate records should be reconciled with paper or electronic records within a 48hr period.

11.4 Posting person identifiable information
11.4.1 External. Precautions need to be taken when sending any confidential or person identifiable information through the external post. This includes clinical records and documentation relating to complaints. Consideration should be given to the method of delivery to ensure that a tracking record is available.

11.4.2 Internal. Confidential or person identifiable information documents such as clinical records, complaints sent internally should be put in an envelope strong enough to take the contents and placed in a courier bag with a seal tab (tamper proof wallet / red bag). The envelope needs to clearly state the recipient and their full address, avoid abbreviations. The recipient of the document should inform the sender that the document has arrived. In addition, where the recipient has not received the documents on time this should be flagged with the sending department. See Internal Confidential Courier Service ("Red Bag" Scheme) **APPENDIX 5 Internal Confidential Courier Service** for more details.
11.5 Faxes and electronic information

Does your fax contain patient information or other confidential information? e.g. patient names, addresses/telephone numbers, dates of birth, diagnosis, treatment, etc

- Yes
  - No special requirements, send as usual
  - No

Are you faxing to a ‘Safe Haven’ fax machine? A Safe Haven fax machine is kept in a room that is locked out of hours or when empty, and faxes received by it are not viewable by members of the public attending the building

- Yes
  - Preferably use a pre-programmed number. If not available on the sending fax, double-check the recipient’s number before using the ‘send / transmit’ key
  - Request the sending machine to produce a transmission report sheet to confirm delivery
  - Telephone the recipient of the fax or their representative to let them know you will be sending confidential information
  - Ask if they would wait by the fax machine while you send it
  - Ask if they would acknowledge receipt of the fax
  - Ensure a cover sheet is marked private and confidential and states who it is for
  - Do not include patient name or clinical details on cover page
  - Double-check the number before using the ‘send / transmit’ key
  - Request the sending machine to produce a report sheet to confirm delivery
  - Remove the fax from the machine, confidential faxes must not be left lying around for unauthorised staff to see
11.6 Emails are covered by the Information Security Policy and the Email and Internet Policy. It should be understood however, that e-mail constitutes an official record when it is sent or received in connection with the transaction of the Trust’s business.

11.7 Clinical records involved in Service user Transfer and Discharge

11.7.1 Service users’ acute trust health records must be transferred with the service user when a service user moves from the acute hospital to the community hospital. This enables health professionals to have access to the full health record and allows them to form decisions based on the individual’s circumstances.

11.7.2 If the service user is transferred without their health records then there needs to be an agreed process by which the notes will be transferred as soon as possible.

11.7.3 Discharge Summary/Plans must contain relevant information and need to be locally agreed and developed to ensure good communication between health professionals, service user and carer.

11.7.4 Acute Trust records must be promptly returned to them once the service user is discharged from the community hospital.

11.8 Retention and disposal schedule of clinical and non-clinical records.

11.8.1 The Trust are responsible for ensuring all files, both electronic and paper, are culled on a regular basis (at least annually) to ensure only active records remain on file and inactive documents are either archived or confidentially destroyed (by shredding or incineration). It is the responsibility of each Manager to ensure local procedures are in place.

11.8.2 Clinical records need to be archived as per the guidance in Records Management: NHS code of practice Part 1 (2006)

11.8.3 The schedule for retention and disposal identifies minimum retention periods. Records Management: NHS Code of Practice (2009) Part 2. Some items may be considered for permanent preservation and the advice of the Company Secretary of an appropriate place of deposit obtained.

11.8.4 It is essential that all documents which relate to an incident and its response are preserved. For these purposes documents also includes notes, log books, flipcharts, photographs, audio and video recordings and information held electronically, including emails as well as any documents that may have been spoilt or defaced. Any clinical records will be
kept in the clinical department in accordance with standard practice.

11.8.5 These documents will be used in the preparation of a formal incident report and may also be called upon at a future date to provide evidence of the trust’s response to any subsequent inquiries such as a public inquiry, coroner’s inquiries and civil litigation.

11.8.6 Services should have records of where all their files are stored and be aware of the retrieval mechanism for these. Staff should contact the Compliance Manager at Trust HQ for retrieval of any off site patient records and the Company Secretary for any centrally archived corporate records. For further details please see APPENDIX 4 Archiving Procedure and Process for Retrieval of Records

11.8.7 The Trust Electronic records are automatically backed up.

11.8.8 It is particularly important for all managers to be aware of the categories of records that are necessary for the Trust to retain. The Trust is not an official “Place of deposit” for permanently preserved records and thus is not required to employ a professional archivist to manage the process of archiving. (Records for permanent preservation are lodged with the local records offices at Bedford and Hertford as “official accessions”). Although the Trust takes on the main responsibility for corporate archiving, “in practice all staff are responsible for any records which they create or use. This responsibility is established at, and defined by, the law. Furthermore, as an employee of the NHS, any records which are created are public records”.

11.8.9 Certain categories of records within the Trust and associated organisations remain the responsibility of the appropriate Director, e.g. Finance, Human Resources, Information Governance Group with input/advice from the Compliance Manager if required.

11.8.10 The document retention requirements may vary depending on the type of incident and the Trust’s involvement so the lead officer will be responsible for ensuring that the Incident lead is made aware of the correct procedures and that they are followed.

11.8.11 for further details and advice, contact:

Compliance Manager
Unit 1 A Howard Court
14 Tewin Rd
11.9 Personal Documents

11.9.1 It is recognised that staff will occasionally use their work computers for their own personal use, which is for material not related to the Trusts business. Storage of such material is not encouraged but if such material is stored, this should be stored on a personal network drive and not on the Trust server. It must be understood that this information is the responsibility of the individual and is not secured or backed-up.

12.0 Access and Recovery

12.1 There is limited access to service user/corporate information due to facilities being closed out of hours. If information is required in an emergency it may be possible to contact the Director on call.

12.2 The IT Service is responsible for ensuring all electronic systems function according to their purpose and are upgraded in line with the manufacturer’s recommendations and the Trusts Business and Continuity Plan. If the system becomes unavailable without notice, the Access and Recovery procedure should still be implemented and all reasonable attempts taken to restore functionality to the computer system as soon as possible. Report any discrepancies to the IT Service desk who will locate the record and return it to the correct database.

12.3 Service user access to records

12.3.1 Service Users in the Trust must be informed at the onset of their care that it is the Trust’s policy to maintain care records and that information is held about them electronically and on paper. Service users must also be informed that information will be shared with other staff and health professionals if professionally required and that some anonymised data may
be used for reporting and ongoing service development purposes.

12.3.2 Service users and non NHS staff should not be given a password or access to the EPR system. However, staff are encouraged to share information in the care records with the service user, where appropriate, and to gain their agreement about what is recorded. Hand held records can be accessed by service users but their entries need to be formally registered by the health professional and actions taken.

12.4 Refer to the Department of Health for full guidance on Access to Records [Dept of Health Guidance on Access to Records 2010 (3).pdf](#)

12.5 Recognised applicants

12.5.1 The Trust will recognise under the above legal provisions the right to access by:

(i) the service user in person; provided that he or she is of an age and capacity to understand the documents.

(ii) a person with ‘parental responsibility’, as defined in the *Children Act 1989* this is a person who has the right to apply for access to a child’s health record as parental responsibility includes safeguarding and promoting the child’s health, development and welfare. It is subject to a declaration by the parent that the child is not of sufficient age or mental capacity to understand. The law regards 16 to 17 year old children adults for the purpose of consent to treatment and right to confidentiality. In some cases a child under 16 who has the capacity and understanding to make decisions about their own treatment are also entitled generally to decide if personal information is passed on (see *Fraser Guidelines Consent to Examination or Treatment Policy*).

(iii) the interests of the parent should be compatible with those of the child. If there is a possibility of serious harm to either the child or a third party by allowing access, the Trust can refuse access.

(iv) an agent, such as a legal representative acting for a service user or client, subject to receipt by the record-holder of a duly signed and dated declaration from the service user/client consenting to disclosure of the records to a third party.

(v) when the service user or client has died, that person’s ‘personal representative’ or anyone who may have a claim arising out of the death. The person’s representative is an executor of the will or an administrator if there is no will and a family member.
(vi) former service users who are now living outside the UK and who have previously been treated in the UK are entitled under the Data Protection Act 1998 to have the same rights to apply for access to their UK records as any person living in the UK.

(vii) if an adult is unable to give consent because they are physically and mentally incapacitated, their next of kin i.e. son or daughter may have access to their health records on request if they have Health and Welfare Lasting power of attorney or the appropriate health professional will consider the request in line with the service user’s best interest and make the final decision to disclose data under Section 60 of the Health and Social Care Act 2001.

(viii) formal requests for access to care records by the service user or their representative must be made in writing to the access to records co-ordinator. The access to records co-ordinator shall ensure the health professional has checked the service user’s health records, as under the Data Protection Act 1998 the Trust may limit or deny access to an individual’s health record request for one or both of the following two reasons:

(ix) where the information released may cause serious harm to the physical or mental health or condition of the service user, or any other person.

(x) where access would disclose information relating to or provided by a third person who had not consented to that disclosure.

12.6 The process for access to records is outlined in the Access to Health Records Policy. Checklist attached as APPENDIX 6 Access to Health Records Checklist

12.7 Hertfordshire Community NHS Trust Designated Data Controller

12.7.1 Company Secretary
Hertfordshire Community NHS Trust
Unit 1A Howard Court,
14, Tewin Court,
Welwyn Garden City,
Hertfordshire
AL7 1BW

12.7.2 The Access to Records coordinator maintains a log of requests to access health records which record the following:

- Forename
- Surname
• Date of Birth
• Address
• Date of request and date of payment
• Authorisation and any associated legal paperwork

12.8 Fees

12.8.1 See table below:

The fees charged by Hertfordshire Community NHS Trust are as per the table below.

<table>
<thead>
<tr>
<th>(a)</th>
<th>For copies of records</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Health records held totally on computer</td>
<td>£10.</td>
<td></td>
</tr>
<tr>
<td>Health records held in part on computer and in part manually:</td>
<td>£40</td>
<td></td>
</tr>
<tr>
<td>Health records held totally manually:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(i) Paediatric or Neurological records</td>
<td>£50</td>
<td></td>
</tr>
<tr>
<td>(ii) Other records</td>
<td>£40</td>
<td></td>
</tr>
</tbody>
</table>

All charges include postage and packaging costs by special delivery

<table>
<thead>
<tr>
<th>(b)</th>
<th>To view records only</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health records held totally on computer:</td>
<td>£10</td>
</tr>
<tr>
<td>Health records held in part on computer and in part manually</td>
<td>£10</td>
</tr>
<tr>
<td>Health records held manually</td>
<td></td>
</tr>
<tr>
<td>(*) unless the records have been added to in the last 40 days in which case viewing is free</td>
<td>£10 (*)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>(c)</th>
<th>To view and receive copies of records</th>
</tr>
</thead>
<tbody>
<tr>
<td>As per (a) above</td>
<td></td>
</tr>
<tr>
<td>(ie There is no combined charge for copies plus viewing)</td>
<td></td>
</tr>
<tr>
<td>NB The Trust reserves the right to waive or refund charges in certain exceptional circumstances and at its absolute discretion</td>
<td></td>
</tr>
</tbody>
</table>

12.8.2 Fees may be waived at the appropriate manager’s discretion, for example, it may be considered inappropriate to charge if the manager is dealing with a complaint and having a debrief with the service user. A Service user is not charged to view their notes if an addition has occurred within the last 40 days.

12.9 Freedom of Information (FOI)

12.9.1 The Freedom of Information Act 2000 gives the public a general right of access to various classes of information held
by public authorities. Published documentation is available on the Trusts website at http://www.hertschs.nhs.uk/freedom-of-information.aspx

12.9.2 Requests for access to documentation that is not published must be made in writing. Please see Hertfordshire Community NHS Trust Publication Scheme and Hertfordshire Community NHS Trust Freedom of Information Policy, FOI Policy for more information.

13.0 Education and Training

13.1 This policy requires training categorised as Priority 1 Mandatory training as identified within the Education, Training & Development Policy s 8. The following table identifies the specific Training Needs analysis for this policy and informs the relevant Risk Management training framework (Education, Training & Development Policy s 9.2).

<table>
<thead>
<tr>
<th>Mandatory Requirement</th>
<th>Session Title</th>
<th>Clinical Staff</th>
<th>Non-Clinical Staff</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Governance</td>
<td>Corporate Induction Information Governance Induction</td>
<td>Induction</td>
<td>Induction</td>
</tr>
<tr>
<td>(including health record keeping)</td>
<td>Information Governance Online Training Tool or marked assessment</td>
<td>Information Governance Refresher Annually</td>
<td>Information Governance Refresher Annually</td>
</tr>
</tbody>
</table>

13.2 This policy will be available for reference for all staff at all times and the Trust will ensure all staff implementing this policy have access to appropriate implementation tools, advice and training. Please see Appendix 7 Mandatory Training Framework for further information.

13.3 The Processes identified within the Education, Training & Development Policy will be used for:

- development of an annual Training Needs Analysis
- development and Implementation of an annual Training Plan
- reporting, monitoring and follow up of staff that fail to complete the mandatory training requirements
13.4 At Induction and appraisal, the line manager and/or appraiser will assess knowledge gaps and agree a personal development plan of how these gaps will be overcome. Where training is required, this will be included within the Departmental Training Needs Analysis so that appropriate training programmes can be commissioned to meet organisational needs.

13.5 The principles of Good Record Keeping are provided as part of the Induction programme. Managers should make staff aware of the need to read relevant policies and procedures, and who the relevant contacts are. This is facilitated by the local induction checklist, which requires that the following are explained by the end of the first week of employment.

(i) Information Governance
   • Information Security Policy
   • Information Governance Policy
   • Records Management and Information Lifecycle Policy
   • Email and internet policy
   • Guidance for Producing Information for Patients

(ii) Clinical Record Keeping
   • Completing Patients Record
   • Paper
   • Electronic
   • Core Data Set

(iii) Further details are available in the Induction Policy

13.5 Requirements for monitoring follow up of non attendance or failure to book required training. Please reference the Education, Training & Development Policy and the Induction Policy.

14.0 Implementation and Monitoring of Compliance

14.1 It is the responsibility of those named in Part (C) of Document History and Control to put into effect the implementation plan

14.2 Monitoring arrangements are specified in Schedule 2.

15.0 Reviewing, Updating and Archiving

15.1 Review of this policy shall be conducted by Compliance Manager, as Lead Officer.
15.2 The date of first review and subsequent review frequency for this document is as prescribed on the cover sheet.

15.3 Details of any amendments shall be recorded by the Lead Officer in Document History and Version Control (E).

15.4 The review, updating and archiving process for this policy shall be carried out in accordance with the Policy for Procedural Documents.

16.0 Interpretation

16.1 In case of doubt, the definitive interpretation of the meaning of any of the content of this policy shall rest with the Lead Director.

17.0 References and Associated Documents


- Consent to Examination or Treatment Policy (2010), Hertfordshire Community NHS Trust. Available from: Consent to Examination and Treatment Policy [Accessed June 2013]
• **CQC Essential Standards of Quality and Safety Outcome 21 Regulation 20** (2009), Care Quality Commission. Available from: [CQC standards](http://cqcstandards) [Accessed June 2013]


• **NHS Code of Practice on Confidentiality** (2003), Department of Health. Available from:

- **NHSLA Standard 1 Criterion 1.7 and 1.8** Available from: CQC NHSLA Standards 2012 - 2013 [Accessed June 2013]


- **Setting the Record Straight** (1995), Audit Commission Available from: Policies\Setting the record straight - Audit Commission.mht [Accessed June 2013]


### 18.0 Document Checklist

### 18.1 The Document Checklist as per Schedule 3 Document Checklist shall be completed by the Document Lead Officer prior to approval by the Designated Committee.
19.0 Equality Impact Statement and Assessment

19.1 Hertfordshire Community NHS Trust is committed to being an organisation within which diversity, equality and human rights are valued. We will not discriminate either directly or indirectly and will not tolerate harassment or victimisation in relation to gender, marital status (including civil partnership), gender reassignment, disability, race, age, sexual orientation, religion or belief, trade union membership, status as a fixed-term or part-time worker, socio-economic status and pregnancy or maternity.

19.2 The Equality Impact Assessment for this policy is attached as Schedule 4 Equality Impact Assessment.
Appendix 1 Guidance on the Maintenance of Personnel Files

GUIDANCE ON THE MAINTENANCE OF PERSONNEL FILES

Contents

1. Introduction 44
2. Scope of Guidelines 44
3. Legislation 44
4. Responsibilities 45
5. Other Policies 45
6. Review 45

Procedure

1. Introduction 46
2. Storage 46
3. New Employee files 46
4. Maintenance of Personnel Files 46
5. Disclosure of Personal Information 48
6. Access to records 48
7. Leavers 50

APPENDICES

A. Tracer Form 51
B. Request to Inspect a Personnel File Form 53
C. Leaver Summary sheet 53
MAINTENANCE OF PERSONNEL FILES

1. Introduction

1.1 Hertfordshire Community NHS Trust (HCT) is committed to ensuring that personnel records held in relation to staff employed by them are kept in accordance with relevant legislation and good practice.

2. Scope

2.1 These guidelines apply to the records held, both paper and electronic, for all staff employed by HCT (whether paid or unpaid) and all applicants for job opportunities within HCT.

2.2 The guidelines do not apply to patients or service users.

3. Legislation

3.1 Relevant legislation includes:-

- Data protection Act (1998) revised 2007
- The Data Protection (Processing of Sensitive Personal Data) Order 2000
- The Privacy and Electronic Communications (EC Directive) Regulations 2003
- The United Kingdom Data Protection (Processing of Sensitive Personal Data) Order 2006

3.2 Main principles of the legislation:-

3.2.1 The type of information covered by this legislation includes paper and computerised records.

3.2.2 Employees have the right to request access to information held regarding them.

3.2.3 Employees and applicants are covered by this legislation.

3.2.4 Data must be:-

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive and must be accurate
- Not kept for longer than is necessary
- Processed in line with Human Rights legislation
- Secure
- Not transferred to countries outside the EU without adequate protection.
4. **Responsibilities**

4.1 All staff have a responsibility to inform their manager of any changes to their personal information, as soon as is reasonably possible. It is a legal requirement that any staff employed under a work permit or sponsorship licence must notify the organisation immediately of any changes.

4.2 All staff that have access to personnel records are required to treat all data in a confidential manner – see Code of Conduct in respect of Patient and Staff Confidentiality.

4.3 All managers who are responsible for personnel records for their staff are required to keep those records in a secure and well maintained condition, in accordance with the legislation above.

4.4 Breaches of this policy may result in disciplinary action.

5. **Other Policies**

5.1 Other policies that should be referred to in conjunction with this guidance are:–

- Information Security Policy
- Information Governance Strategy

5. **Review**

This document will be reviewed after two years or earlier at the discretion of the Lead Director.
PROCEDURE

1. **Introduction**

1.1 This procedure covers how personnel files are to be stored and maintained, as well as the procedure for staff to request access to their own records.

2. **Storage**

2.1 All personnel files should be kept in secure place. Paper files should be kept under lock and key. Any information on staff held in computerised form must be held in a secure location with secure access control. Only staff with the proper authorisation should have access to personnel files.

2.2 It is good practice to keep any information that is of a sensitive nature such as sickness records separate to less sensitive information. They could be kept in a paper envelope within the personnel file.

3. **New Employee Files**

3.1 New Employee Files should contain the following documents:

- Copy of Job Advert
- Job Description
- Person Specification
- Application Form / CV / supporting application information
- Interview Notes
- Conditional Offer
- Formal Offer Letter
- Copies of references (in a sealed envelop)
- Notification of Staff Health Assessment
- Copy of acceptance letter
- Copy of IAT request (if applicable)
- Granting Incremental Credit Form (if applicable)
- Copies of Passport
- Qualification Information
- Copy of Payslip
- Copies of Proof of Eligibility to Work
- Copy of signed contract of employment

It will not contain the following:-

- Equal Opportunities Monitoring Form
- CRB Disclosure Check
- Pre-employment Health Questionnaire

4. **Maintenance of Personnel Files**

4.1 All Managers who have responsibility for staff should ensure that they have adequate and secure filing facilities for personnel records. These facilities do not have to be within the Manager’s own office but must be secure at all times.
4.2 Managers must ensure that all staff who have access to personnel records understand their responsibilities within this policy and that personnel information is handled with respect.

4.3 If a file is removed from its normal storage system for any reason, a Tracer Form (Appendix A) should be completed to enable the file to be safely returned to the filing system. Absent records should be regularly chased for their return. The Records Management and Information Lifecycle policy and procedure also contains information on tracking the movement of information and tracing records.

4.4 Any health information collected will be subject to the Data Protection Act and therefore it is important to ensure that there is a justifiable reason for requesting this information. An employee has the right to privacy and can deny access to his / her medical data. It is also essential to keep health information secure and should be kept separate to less sensitive information. Most of the health information relating to HCT employees would be held by Occupational Health under similar conditions.

4.5 The Line Manager should review the information kept on the personnel file annually to ensure that any information that is irrelevant, excessive or out of date is destroyed in a confidential way.

4.6 The following should be kept on personnel files:-

- Original Job Advertisement Form
- Job Description
- Person Specification
- KSF Outline
- Copies of proof of ID
- Copies of proof of registration where applicable
- Copies of letters confirming Leave to Remain or Copies of work permits where applicable
- Copies of examination certificates where applicable
- Application Form
- Letter offering employment
- Copy of acceptance letter
- Appointment form/ new starter form
- Copy of Granting Incremental credit request where applicable
- References
- Notification of staff health assessment
- Contract of Employment
- Variations of Employment letters
- Copies of Change of Circumstance forms
- Special Leave Request Forms
- Current Disciplinary Warnings including notes of informal warnings
- Current Attendance Management Warnings including notes of informal warnings
- Any current letters, notes or Action plans relating to the Capability policy Grievances and Complaints
- Current Training Certificates
• Complaints about the employee – this can be kept up to a year as long as the complaint was shown to the employee and they have had the opportunity to respond. Any response should also be documented. If there is no record of the complaint being discussed with the employee, then it should be destroyed.
• Annual leave
• Sickness Certificates and Medical Reports – these should be kept in a sealed envelope and should only be kept for as long as the report remains relevant.
• Maternity paperwork
• Accident Report forms
• Return to Work interview paperwork
• Termination (Leaver) Paperwork

(This list is not exhaustive or exclusive)

IF THERE ARE ANY DOUBTS ABOUT REMOVING ANY PAPERWORK FROM A PERSONNEL FILE, CONTACT THE HR DEPARTMENT FOR ADVICE.

4.7 The following should not be kept on personnel files:-

• Expired Warnings
• Expired Informal warnings.
• CRB Disclosure Check
• Pre-employment monitoring – Health Questionnaire or Equal Opportunities monitoring form.

(This list is not exhaustive or exclusive)

5. Disclosure of Personal Information

5.1 The employee’s permission must be given before any disclosure may be made, unless there is a legal requirement to disclose that information (e.g. in criminal or tax investigations or where legal action is involved).

5.2 The source of all requests for personal information must be checked for authenticity.

5.3 All disclosures should be relevant to the information requested and give no further information than that requested.

5.4 Any disclosure of personal information must be checked by an appropriate senior manager before being disclosed.

6. Access to records

6.1 Under the Data Protection Act 1998 all employees have
- a right to information about the data held and access to it
- a right to object to use of the data
- a right to seek correction, deletion and destruction of inaccurate information
6.2 All information on files will be available for individuals to see except for those items listed below:

- Outgoing references: Under the Data Protection Act, an employer does not have to provide a copy of a reference; however, it would be reasonable to provide a copy of a reference as it should only contain factual information.
- Incoming references marked “confidential” – The referee should be contacted to obtain their permission before disclosing the reference. If the referee refuses, then contact the HR Department for further advice.

NB There is no need to retain references indefinitely after appointment. The Line Manager should arrange for these to be destroyed after twelve months unless the terms of the appointment require retention for a longer period.

6.3 Procedure for employee to request to see their personnel file:

a) Employees wishing to access their personnel files should be asked to complete the request form (Appendix B) and send it to the Human Resources Department.

b) Upon receipt of the completed form the HR Department will write to the employee giving the employee an appointed time to inspect the file and the name of the authorised manager dealing with the matter. (This is to avoid employees calling into the office on a casual basis.)

c) The authorised manager must comply with a request promptly and in any event within thirty days of receipt of the request.

d) The information given in response to a request should be all that is contained in the personnel file at the time when the request was received. Routine amendments and deletions of the information may continue, but there should be no special amendments or deletions that would not otherwise been made.

e) Before allowing access to the personnel file the identification of the employee must be confirmed by the authorised manager through a means of identification.

f) Confidential references to and from the Trust and any other information relating to a third party, who can be identified from that information, where an express refusal of consent has been given by the individual, should be temporarily removed prior to access being granted.

g) The authorised manager should remain with the employee whilst the file is being inspected.

h) If the employee requests photocopies of documents on the file the authorised manager should make the copies and make note that these have been provided to the employee. The individual should not be left alone with the file whilst the photocopies are being made.

i) A record of all access requests should be held and checked no an annual basis by the authorised manager to ensure employees do not make and excessive number of requests.

j) Employees have the right to be accompanied by a representative of a trade union or professional organisation, or colleague not acting in a legal capacity, when inspecting their file and should be informed of this.

Objection to processing

a) If the employee disagrees with the inclusion or content of any document or questions why a document is not held, she/he should be
asked to register the objection in writing and told the name of the manager who will consider the matter.

b) Employees who have disagreed with the judgement given by this manager have the right to pursue the matter through the Grievance Procedure. They should be informed of this.

c) An employee can require the Trust to cease or not to begin using any personal data about him or her on the grounds that it is likely to cause substantial damage or distress to him or her or another and such damage or distress would be unwarranted.

d) In this situation an employee may serve notice on the Trust requiring the cessation of using that information. Upon receipt of this notice a reply must be given within 21 days that the request will be met or giving reasons why, or to what extent, the request will be refused.

e) This provision does not apply where the employee has given consent to using the information, it is necessary for the performance of his or her contract or it is necessary for compliance with a legal obligation.

f) Where a request is refused, the employee may appeal and to an Employment Tribunal when internal procedures have been exhausted, e.g. Grievance Procedure.

7. **Leavers**

7.1 The Line Manager should ensure that Personnel files are kept for up to six years after the individual has left or the individual’s 70th birthday, whichever is the later.

7.2 The Line Manager should then ensure that the Leaver Summary Sheet (Appendix 3) should be kept for 30 years. However, Industrial Relations paperwork should be kept for 10 years and Nurse Training records should be kept for 30 years. The documents should be kept in a secure location.

7.3 The Line Manager should ensure that the following process is followed on receipt of a resignation letter:
   - Complete the Leaver Summary Sheet (Appendix C)
   - Place in a plastic folder and attach to the front of the Leaver file.
   If there is Industrial Relations paperwork or Nurse Training Records, these should be placed in the plastic folder together with the other information listed on the summary sheet.

7.4 Once the six years have been reached or the individual’s 70th birthday whichever is the later, then the Line Manager can arrange for the main file to be destroyed under confidential conditions. The summary sheet should be kept for 30 years.

7.5 The Records Management and Information LifeCycle Policy and Procedure contains information on the process for Archiving, retrieval and destruction of records.
## TRACER FORM

TO BE COMPLETED EVERY TIME THE FILE IS REMOVED FROM FILING

<table>
<thead>
<tr>
<th>Date:</th>
<th>Name of Person Removing</th>
<th>Name of Document</th>
<th>Location and Person sent to</th>
<th>Date/Method Confirmed receipt</th>
<th>Date File Returned</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
REQUEST TO INSPECT A PERSONNEL FILE

Name .................................................................

Job Title ............................................................

Section ...............................................................

Department .........................................................

Signature ......................................................... Date

Notes:-

1. Inspection of files will be by appointment only.

2. You have a number of rights in relation to your personal record which are; the right to information about the data held and access to it, a right to object to use of the data and a right to seek correction, removal and destruction of inaccurate, or out of time, information.

3. You will be required to bring with you some form of personal identification.

4. An authorised manager will be present whilst you look at your file.

5. You will not be permitted to remove anything from the file. If you wish to copy any of the contents you must inform the authorised manager who will arrange it for you.

6. You will not be permitted to see confidential references to or from the Trust.

7. If you have any objection to the information held this should be a taken up in the first instance with the manager dealing with this application. If the matter is not resolved to your satisfaction you have recourse through the Grievance Procedure to pursue the issue.

8. This completed form should be sent to your Human Resources Department.

9. The Human Resources Department will write to you with details of an appointment.
# LEAVER SUMMARY SHEET

<table>
<thead>
<tr>
<th>NAME OF EX-EMPLOYEE</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>NAME OF ORGANISATION</td>
<td></td>
</tr>
<tr>
<td>POST TITLE</td>
<td></td>
</tr>
<tr>
<td>BASE</td>
<td></td>
</tr>
<tr>
<td>LINE MANAGER</td>
<td></td>
</tr>
<tr>
<td>BAND</td>
<td></td>
</tr>
<tr>
<td>HOURS</td>
<td></td>
</tr>
<tr>
<td>DATE STARTED</td>
<td></td>
</tr>
<tr>
<td>DATE LEFT</td>
<td></td>
</tr>
<tr>
<td>BIRTH DATE</td>
<td></td>
</tr>
<tr>
<td>CONTINUOUS SERVICE</td>
<td></td>
</tr>
<tr>
<td>WITH NHS</td>
<td></td>
</tr>
<tr>
<td>REASON FOR LEAVING</td>
<td></td>
</tr>
<tr>
<td>DESTINATION ON</td>
<td></td>
</tr>
<tr>
<td>LEAVING</td>
<td></td>
</tr>
<tr>
<td>SICKNESS IN LAST</td>
<td></td>
</tr>
<tr>
<td>YEAR BEFORE LEAVING</td>
<td></td>
</tr>
</tbody>
</table>

Documents to be kept if applicable:
- Industrial Relations paperwork
- Nurse Training Records
CONFIDENTIALITY STATEMENT AND AGREEMENT

To be completed by agency, temporary, voluntary, consultant, contracting and other people who are not employed by the Trust under a contract of employment but who may have access during the course of their responsibilities, role or commission, to confidential information. This includes people other than Trust employees who may serve on Trust committees or working groups.

Agency, temporary, voluntary, consultant, contracting and other personnel who are not employed by the Trust under a contract of employment, are requested to read and agree to the following conditions regarding confidentiality of client, staff and commercial information.

This applies to confidential information which may be acquired by any means during the course of their work, role or commission with the Trust.

All people working for or on behalf of the Trust must at all times be aware of the importance of maintaining confidentiality of information gained by them during the course of their duties. This will in many cases include access to personal information relating to patients or clients. All information must be treated and processed in a discreet and confidential manner, and particular attention is drawn to the following:-

1. Information regarding patients or clients must not be disclosed orally, in writing or by any other means to unauthorised persons. It is also particularly important to ensure that persons making telephone enquiries about patients or clients are entitled to receive personal information.

2. Written records, computer records and correspondence pertaining to any aspect of the Trust’s activities must be kept secure from unauthorised access at all times.

3. If relevant, you have an obligation to ensure that computer systems which you use are protected from inappropriate access within your direct area of practice e.g. by ensuring that they are protected by a personal access password and that this kept secure.

4. All data held, its management and procedures must conform to the requirements of the Data Protection Act (1998) to ensure that the Trust holds and processes data “fairly and lawfully” under the Act. Service users and staff also have a right to access their records on application to the appropriate manager.
5. If it is appropriate and necessary to share information gained in the course of your work with health or social work practitioners, you must make sure that, as far as is reasonably possible, this information will be kept in strict professional confidence and be used only for the purpose for which the information is provided.

6. Conversations relating to confidential matters affecting patients, clients, staff or commercial interests should not take place in situations or locations (on or off Trust premises) where they can be overheard by persons not entitled to be in receipt of that information, e.g. in corridors, reception areas, and public areas.

7. Confidential information affecting patients, clients, staff or commercial interests must not be shared with family members, friends or any other person not entitled to be in receipt of that information.

8. The obligation to maintain confidentiality in respect of confidential information acquired whilst working for or on behalf of the Trust extends for an indefinite time period after the work for or on behalf of the Trust has ceased.

9. Any breach of confidentiality may be regarded as misconduct or gross misconduct and may, subject to the nature and extent of the breach, result in termination of any arrangement by which a person works for or on behalf of the Trust or in extreme cases, formal legal action being pursued.

10. Doubts or queries about whether information is deemed to be confidential or whether confidential information may be disclosed in any specific circumstances should be referred to the sponsoring manager, in the first instance. The sponsoring manager for this purpose is the Trust Officer who has commissioned or who supervises your role with the Trust. Your sponsoring manager is:

   (Name, Title and address)
   Tel. No. E-mail address:

I confirm that I have read, understood and agree to comply with the above conditions.

Name (Block Capitals) .................................................................

Signature .................................................................

Role .................................................................

(Date) .................................................................

Please complete and return to your sponsoring manager (details as above):
Appendix 3 Core Content in clinical records

- Service user’s full name or known as and any known aliases
- Postcode and full address (use postcode look-up facility to insert address)
- Telephone number(s)
- National Health Service Number
- Date of birth
- Gender
- Civil/Marital status (unless service user declines to give this information)
- Next of kin or agreed contact as identified by service user
- Named carer where appropriate
- Parent or guardian where appropriate
- Advocate where appropriate
- Details of General Practitioner
- Religion where appropriate (unless service user declines to give this information)
- Diagnosis
- Medication
- Any allergies, this includes any food allergies, such as potato or kiwi fruit as it can indicate a potential allergy to latex. This should be documented in the document’s inside cover in a designated place
- Advanced decisions are documented in a clearly designated area on the document’s inside cover
- Details of the ethnic group to which the service user wishes to be assigned (unless service user declines to give this information)
- First language if not English (with details of need for interpreter)
- Communication needs if there is sensory loss, e.g. signing
- Disability
- Employment
- Consent to treatment Refer to Consent to Examination or Treatment Policy
- Consent to Information Sharing. Refer to the eDMS operational policy on SystmOne webpage
- The clinical record must contain information relevant to professionals involved in the care of the service user. Assessment outcomes should be readily identifiable as should decisions made and information given to service users
- Needs/problems the service user is experiencing and suggested actions, the treatment and/or care to be provided and a review date or plan of further action, including the agreed next contact point, by whom, how and where
- Relevant information regarding the health status (mental, social and physical) of the service user at any given time and the practitioner’s response to identified needs.
- The event/contact the clinical note refers to. A scheduled appointment or event should be created against each clinical entry where a telephone or face to face meeting with the service user, their representative, or another professional has taken place.
• All telephone consultations and emails where advice and information is offered should be recorded in the care record as a clinical note if clinically relevant.
• The name of any leaflets, the version and edition number and the date given to the patient should be recorded. The leaflet should be filed in the patient paper record.
• Patient’s key safe information should **not** be entered on SystmOne. The practice is unsafe because it then becomes available to anybody who has access to the record either within their own SystmOne unit or through another unit as the record is being shared. This information should be recorded in work diaries together with the patient’s initials and without reference to this being key safe information.
Appendix 4 Archiving Procedure and Process for Retrieval of Records

Record systems maintained by Trust staff must provide timely and efficient access to, and retrieval of, records needed in the continuing conduct of business and to satisfy related accountability requirements.

The Hertfordshire Community NHS Trust has a contract for archiving paper documentation with an external document storage organisation called Cintas. Responsibility for monitoring the archiving contract lies with the Compliance Manager.

If electronic versions of documents are securely archived then paper copies need not be retained.

The Standard Operating Procedures for Archiving are to be found on the Document Storage page of the intranet.

Standard Operating Process for Archiving

There is a Standard Operating Procedure (SOP) which specifies in greater detail the process for putting boxes of records into storage DS SOP 1

In summary the SOP says that:

HCT Service Department (HCT SD) identifies general requirement for storing records with a commercial document storage company (Cintas) and gains authorisation from their service manager.

SD refers to archiving details which are published on the Information Governance page of the intranet; this includes standards to be adopted and the price list for storage and associated services.

The HCT SD (service department) acquires suitably strong cardboard boxes which ought not to collapse in storage.

The HCT SD boxes up records to the required standard. This will include:

- labelling up the boxes with suitable details including a valid destruction date for the box
- preparing a list of all the records in the box to the required standard
- putting a copy of the list of records in the box and keeping a list on the HCT SD N Drive
- inputting individual record detail to include NHS and DOB onto the Cintas database
If records are not boxed up to the required standard then they will be rejected by the storage supplier.

A bar code readable label should be on each box prior to sending boxes off for storage. This will allow all boxes to be electronically tracked from the time they are initially taken into storage through to their eventual destruction.

Written confirmation of authorisation to archive records is required from the service manager. This can be either by email or in a written form. This should be retained by the service.

HCT SD arranges transport of boxes to archive warehouse, by processing request via Cintas web based system.

**Hints and tips:**

Before starting, consider the logistics and ergonomics of the overall process which includes:

- space to store sufficient flat pack boxes and lids
- space, locations and arrangements for:
  - boxing up records
  - making a list of records which are in each box
  - labelling the boxes
  - recording which records are in the boxes
  - transporting and storage of boxes pending them being picked up by the storage supplier
  - management arrangements for controlling and monitoring the activity of boxing up records
  - arrangements for ensuring valid data entry into the storage suppliers computer system

Identify sufficient time and acquire sufficient resources to do the work. It may take 1.5 hours or so to:

- assemble a box and lid from a flat pack state
- put records into a box
• list the records which are in the box (this is the most time consuming part of the process)

• label up the box

Don’t leave all the work to one individual or leave it to the last moment, once a year. Think about:

• when records are put into a folder/envelope, record data for the list of records on the folder/envelope

• the potential to archive into boxes every 3 or 6 months or having a rolling programme for a service where records for different locations are archived at different times of the year

Don’t put records with significantly different retention periods in the same box e.g. keep records for children separate from records for adults and don’t put HR employee records and patient records in the same box.

Services should attach a storage label to the side of the box to include the information in the table below. The label reference number is Banner 967 0055

<table>
<thead>
<tr>
<th>DEPARTMENT</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>BASE/LOCALITY</td>
<td></td>
</tr>
<tr>
<td>CONTAINS NAME / TITLE OF DOCUMENTS</td>
<td></td>
</tr>
<tr>
<td>STORAGE DATE</td>
<td></td>
</tr>
<tr>
<td>FILLED BY</td>
<td></td>
</tr>
<tr>
<td>REF NUMBER</td>
<td></td>
</tr>
<tr>
<td>DESTRUCTION DATE</td>
<td></td>
</tr>
</tbody>
</table>

**Retrieval**

For retrieval of records please refer to DS SOP 2 - retrieval of records. Note that there is a cost to retrieval from these archives. Costs are outlined in Appendix 1 of SOP 1; SOP 1 - storage of records. Files will be couriered to the location required by a specialist courier within two working days.
Destruction

Please refer to the Standard Operating procedure for the destruction of records and the schedule for records retention and the disposal list.

**DS SOP 3 - Box destruction Dec 12.pdf**

**Schedule for retention and disposal of records.doc**

This retention schedule details a minimum retention period for each type of record. Records, whatever format they may be in, may be retained for longer than the minimum period. Care records should not normally be retained for more than 30 years. When a period of longer than 30 years is required –e.g. preservation for historical purposes or any pre 1948 records, the National Archives should be consulted.

Records containing personal information are subject to the Data Protection Act 1998 and should be handled appropriately.

If you are unsure about disposal and retention dates please contact the Compliance Manager.

Records (including copies) not selected for archival preservation and which have reached the end of their administrative life should be destroyed in as secure a manner as is appropriate to the level of confidentiality or protective markings they bear. This can be undertaken on site or via an approved contractor. Records should be destroyed beyond any possible reconstruction.

Most NHS records are confidential records. Contractors, if used for the destruction of records, should be required to sign confidentiality undertakings and to produce written certification as proof of destruction. Contact the Compliance Manager for the details of contractor(s).

A Record of the destruction of records, showing their reference, description and date of destruction should be maintained and preserved by the Compliance Manager, so that the organisation is aware of those records that have been destroyed and are therefore no longer available. Disposal schedules would constitute the basis of such a record.

If a record due for destruction is known to be the subject of a request for information, or potential legal action, destruction should be delayed until disclosure has taken place or, if the authority has decided not to disclose the information, until the complaint and appeal provisions of the Freedom of Information Act have been exhausted or the legal process complete.
Appendix 5 Internal Confidential Courier Service (“Red bag” Scheme)

Purpose:
To ensure that Hertfordshire Community NHS Trust couriered confidential mail is safely transported between sites.

Contents of Bags
The contents sheet must be completed for every bag. When sending service user notes and confidential documents the correct information should be recorded on the contents form for each individual service user. When sending service user slips, i.e. development checks, MIU slips etc. these can be bundled up and put into one envelope which is recorded on the contents sheets just listing the envelope.

The completed red bag contents sheet is to be placed inside the red bag with the confidential material. Make a copy of the contents sheet and retain until receiving the original back from the receiving unit. This will provide assurance to that the records have been delivered to the intended recipient. The bag is then sealed using a security tag. Bags will not be collected by the courier unless sealed. The completed Tracker Form is then secured to the outside of the bag. Bags should be returned to sender within a one week period.

Numbered White Security Seals:
Come in Box of 500s £8.32 Order via: NHS Supplies Code: WYY207 (costs as at 2010 prices)

Tracker Forms
Complete the tracker form recording all the details as directed on the form. If the transfer route includes a post room please tick the relevant box, if known.

Operating Requirements
1. Trust courier drivers collect or deliver children services secured mail from designated area as per run sheet. Courier drivers collecting mail must sign for it upon collection only if it is in a secured mailing pouch. Courier drivers delivering children services couriered mail must ensure it is signed over to a member of staff at the delivery destination.
2. Driver to sign and date the tracker form on every run.
3. If returning to Lister/QEII for onward travel secured mail pouch (red bag) should be delivered to the post room. A member of post room staff must sign for the secured pouch (red bag) from the driver.
4. If there is no mail personnel in the post room on return from the final run the secured mail pouch (red bag) should be placed in the designated pigeon hole.
5. Drivers must ensure that they sign for any secured mailing pouches that they receive from the post room. Driver will then deliver secured mailing pouch (red bag) to designated delivery point. Upon arrival at destination a member of staff must sign for the secured mailing pouch (red bag) before delivery can be finalised.
Clinical service require to transfer patient notes or other confidential material via courier service to another service department or location in Hertfordshire.

- Seal Bag using security tag
- Complete red bag contents sheet and insert inside red bag with confidential material
- Unit make copy of contents sheet and retain until confirmation of receipt from receiving unit.

- Complete tracker form recording transfer details and seal number
- Bag left at designated collection point for courier
- Courier transports Confidential material
- Confidential material signed for on arrival at end users destination
- Contents checked, red bag and completed contents sheet returned to sender
RED BAG

CONTENTS INSIDE RED BAG

Seal Number: ........................................

Sender Name: .................................  Base: ........................................

Contact Telephone Number: .................  Internal Postal Code: ..............

<table>
<thead>
<tr>
<th>Description/Type of Contents</th>
<th>Name of Service user</th>
<th>NHS Number</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(If any discrepancy is found, please refer back to sender)

Confirmation of receipt: .................................................................

Print Name: .................................................................

Dept: .................................................................

Date: .................................................................

*Now please return this sheet back to the sender in this red bag as confirmation of receipt*
Tracking Form (attach completed form to the outside face of Red Bag before sending)

<table>
<thead>
<tr>
<th>DATE</th>
<th>FROM</th>
<th>TO</th>
<th>BAG SEAL NO</th>
<th>RECEIVED BY</th>
<th>PRINT NAME</th>
<th>SIGNATURE</th>
<th>DATE &amp; TIME</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Appendix 6 Access to Health Records Checklist

The Data Protection Act 1998
This Act gives every living person, or their authorised representative, the right to apply for access to their health records to obtain copies in writing

Are you satisfied that you have consent from the patient and have enough information to identify them and locate the information they require, along with the relevant access fee?

Write back to the applicant with a consent form, to obtain the appropriate information.

Please send the consent form to the Access to Record coordinator at Trust HQ. This Access to Record process is a joint process carried out by the Access to Record coordinator in liaison with the relevant health professional.

Log applicant request and comply promptly.

Ensure the health professional has checked the patient's health records: access may be limited or denied where the information released may cause serious harm to the physical or mental health or condition of the patient, or any other person, and/or where access would disclose information relating to or provided by a third person who had not consented to that disclosure.

As promptly as possible and in any case within 40 days of receipt of the fee payable, either:

• provide the patient or their representative copies of the relevant parts of the health records
or
• inform the patient or their representative that access cannot be granted (deny access)
or
• by agreement with the data controller, set a date for patient or their representative to view the relevant records once the relevant fee has been paid.

If the patient is unhappy with any aspects of the access request, try to resolve locally with the data controller. If this is not an option they should be directed to the Information Commissioner Office.
### Appendix 7 Mandatory Training Framework

<table>
<thead>
<tr>
<th>HCT ESSENTIAL/REGULATORY TRAINING MATRIX</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mandatory Requirement</td>
</tr>
<tr>
<td><strong>Record Management Policy (Information Governance)</strong></td>
</tr>
<tr>
<td><strong>Record Management Policy (Information Governance)</strong></td>
</tr>
<tr>
<td><strong>Record Management Policy (Information Governance) Refresher</strong></td>
</tr>
<tr>
<td><strong>Record Management Policy Induction</strong></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
Schedule 1 Committee Structure/Reporting Flow-Chart (September 2012) For This Policy
## Schedule 2 Document for Compliance Monitoring

<table>
<thead>
<tr>
<th>Minimum Requirements to be monitored</th>
<th>Process for Monitoring Compliance</th>
<th>Responsible Individual/Group/Committee</th>
<th>Frequency of Monitoring</th>
<th>Reported to Designated Committee Review of Results</th>
<th>Development of Action Plan</th>
<th>Monitoring Action Plans and Implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duties</td>
<td>The Policy Lead Officer will review the data collected as below and take into consideration to amend the policy or take forward additional recommendations required to support compliance and safe practice.</td>
<td>Procedural Document Lead Officer</td>
<td>6 monthly</td>
<td>Information Governance Group (IGG)</td>
<td>Procedural Document Lead Officer Update Policy</td>
<td>As per policy review schedule or earlier at discretion of the Lead Director. IGG note review of policy and/or approve new edition. Policy disseminated</td>
</tr>
<tr>
<td>NHSLA 1.7 Health Records Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NHSLA 1.8 Health Record Keeping Standards</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Basic Record Keeping Standards which must be used by all healthcare professionals for</td>
<td>Clinical Record Keeping audit -demographic data including NHS number and ethnicity</td>
<td>Senior Information Risk Owner</td>
<td>Annual</td>
<td>Information Governance Group and CACE</td>
<td>SIRO ensures development of action plan for improvement</td>
<td>Minutes from IGG and CACE note improvements and progress towards</td>
</tr>
<tr>
<td>Process</td>
<td>Activity</td>
<td>Frequency</td>
<td>Responsible Body</td>
<td>Notes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------</td>
<td>----------</td>
<td>-----------</td>
<td>------------------</td>
<td>-------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>the completion of all health records</td>
<td>- contemporaneous including page numbers, entries -attributable -clinically relevant</td>
<td></td>
<td></td>
<td>compliance and lessons learned</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Health Record Keeping Standards 1.8a</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Legal obligations that apply to records</td>
<td>Analysis of incidents relating to IG</td>
<td>Compliance Manager</td>
<td>Quarterly</td>
<td>Information Governance Group</td>
<td>SIRO ensures development of action plan for improvement Minutes from IGG note improvements and progress towards compliance and lessons learned</td>
<td></td>
</tr>
<tr>
<td>Health Records Management 1.7b</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Process of tracking records</td>
<td>Analysis of Information Governance incidents</td>
<td>Compliance Manager</td>
<td>Quarterly</td>
<td>Information Governance Group</td>
<td>IG group ensures development of action plan for improvement through delegated leads Minutes from IGG note improvements and progress towards compliance and lessons learned</td>
<td></td>
</tr>
<tr>
<td>NHSLA 1.7d Health Records Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Process for creating records</td>
<td>Record Keeping audit</td>
<td>Senior Information Risk Owner</td>
<td>Annual</td>
<td>Information Governance Group</td>
<td>SIRO ensures development of action plan for improvement Minutes from IGG note improvements and progress towards compliance and lessons learned</td>
<td></td>
</tr>
<tr>
<td>NHSLA 1.7c Health Records Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Process for ensuring a contemporaneous complete record of care</td>
<td>Clinical Record Keeping audit</td>
<td>Senior Information Risk Owner</td>
<td>Annual</td>
<td>Information Governance Group and CACE</td>
<td>SIRO ensures development of action plan for improvement</td>
<td>Minutes from IGG and CACE note improvements and progress towards compliance and lessons learned</td>
</tr>
<tr>
<td>Process for retrieval of records NHSLA 1.7e Health Records Management</td>
<td>Analysis of IG incidents</td>
<td>Compliance Manager</td>
<td>Quarterly review</td>
<td>Information Governance</td>
<td>IG group ensures development of action plan for improvement</td>
<td>Minutes from IGG note improvements and progress towards compliance and lessons learned</td>
</tr>
<tr>
<td>Process for retention disposal and destruction of records NHSLA 1.7f Health Records Management</td>
<td>Audit of disposal schedules and Information Governance incidents</td>
<td>Compliance Manager</td>
<td>Annual</td>
<td>Information Governance Group</td>
<td>IG group ensures development of action plan for improvement</td>
<td>Minutes from IGG note improvements and progress towards compliance and lessons learned</td>
</tr>
<tr>
<td>Organisation’s expectations in relation to staff training, as identified in the Review Statutory and Mandatory Framework, and Essential and Regulatory</td>
<td>Review Statutory and Mandatory Framework, and Essential and Regulatory</td>
<td>Head of Learning and Development</td>
<td>Annual</td>
<td>Health and Safety Group</td>
<td>Director of Finance and Commerce and Director of HR and OD will</td>
<td>Moments of the Health and Safety Group note progress of improvement</td>
</tr>
<tr>
<td>training needs analysis</td>
<td>Training Framework presented to Health and Safety Group</td>
<td>ensure an action plan is developed for improvement towards compliance</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------------</td>
<td>--------------------------------------------------------</td>
<td>---------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NHSLA 1.8c Health Record Keeping Standards</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Process for monitoring compliance with minimum requirements</td>
<td>Analysis of data in the IGG Annual Report including Information Governance Toolkit</td>
<td>Senior Information Risk Owner</td>
<td>Annual</td>
<td>Board via IGG</td>
<td>SIRO ensures development of action plan for improvement</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Minutes from IGG note improvements and progress towards compliance and lessons learned</td>
<td></td>
</tr>
</tbody>
</table>
Schedule 3 Document Checklist

- To be completed and “signed-off” prior to approval by a person identified by the Lead Officer.

- This shall be somebody who is the Lead Officer for one or more other procedural documents or, in case of difficulty in identifying an appropriate person, it shall be somebody nominated for the purpose by the Company Secretary (for corporate documents) or the Head of Risk & Assurance (for clinical documents).

<table>
<thead>
<tr>
<th>Title of document being reviewed:</th>
<th>Yes/No/Not applicable</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Title</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is it clear whether the document is a policy, procedure or other procedural document?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Rationale</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are reasons for development of the document stated?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Development Process</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you feel a reasonable attempt has been made to ensure relevant expertise has been used?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is there evidence of consultation with stakeholders and users?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Content &amp; Format</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is the document content and format in line with the Guidance Notes: Template For Trust Procedural Documents?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is the objective of the document clear?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is the target population clear and unambiguous?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are the intended outcomes described?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are the statements clear and unambiguous?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
5. **Evidence Base**  
Is the type of evidence to support the document identified explicitly?  
Are key references cited and in full?  
Are supporting documents referenced?  
Does the document meet requirements of regulatory or external / internal assessment bodies as far as applicable (e.g. NHSLA, CQC registration, Information Governance Toolkit, Internal Audit Report recommendations, etc.)

6. **Approval**  
Does the document identify which committee / group / officer will approve it?  
If appropriate have the Joint Negotiating Committee been consulted

7. **Dissemination and Implementation**  
Is there an outline/plan to identify how this will be done?  
Does the plan include the necessary training/support to ensure compliance?

8. **Document Control**  
Does the document identify where it will be held?  
Have archiving arrangements for superseded documents been addressed?

9. **Process to Monitor Compliance**  
Are there measurable standards or KPIs to support the monitoring of compliance of the document?
<table>
<thead>
<tr>
<th>Question</th>
<th>Answer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is there a plan to review or audit compliance with the document?</td>
<td></td>
</tr>
<tr>
<td><strong>10. Review Date</strong></td>
<td></td>
</tr>
<tr>
<td>Is the review date identified?</td>
<td></td>
</tr>
<tr>
<td>Is the frequency of review identified? If so is it acceptable?</td>
<td></td>
</tr>
<tr>
<td><strong>11. Overall Responsibility for the Document</strong></td>
<td></td>
</tr>
<tr>
<td>Is it clear who will be responsible for co-ordinating the dissemination, implementation and review of the document?</td>
<td></td>
</tr>
</tbody>
</table>

**Reviewed By (Name):**

**Post Title:**

**Date:**
### Schedule 4 Equality Impact Assessment

**1. Policy**

<table>
<thead>
<tr>
<th>Title: Record Management and Information Lifecycle Policy</th>
<th>Stage 1 EIA Completion Details</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Names &amp; Titles of staff involved in completing the EIA:</td>
</tr>
<tr>
<td>Existing Date of Completion: 21/06/13</td>
<td>Karen Seikus Compliance Manager</td>
</tr>
<tr>
<td>Review Date: 21/06/15</td>
<td></td>
</tr>
</tbody>
</table>

**2. Details of the Policy. Who is likely to be affected by this policy?**

- [x] Staff
- [x] Patients
- [ ] Public

**3. Impact on Groups**

<table>
<thead>
<tr>
<th>Probable impact on group?</th>
<th>Positive</th>
<th>Adverse</th>
<th>None</th>
<th>High, Medium or Low Impact</th>
<th>Please explain your answers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Race, ethnicity, nationality, language etc.</td>
<td></td>
<td></td>
<td>❌</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gender (inc. gender recognition)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disability, inc. learning difficulties, physical disability, sensory impairment etc.</td>
<td></td>
<td></td>
<td>❌</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sexual Orientation, including gay, lesbians, transgender</td>
<td></td>
<td></td>
<td>❌</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Religion or belief</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Human Rights</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Age</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other: please state</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**No impact on any of the groups above.**

There is unlikely to be an adverse impact on different minority groups

**4. How could the identified adverse effects be minimised or eradicated?**

**5. How is the effect of the policy on different Impact Groups going to be monitored?**

**6. Please demonstrate what research and consultation methods evidence you have to support your policy.**