Camden and Islington NHS
Mental Health and Social Care Trust

RECORDS MANAGEMENT POLICY

Mar 2007

Camden ISLINGTON
supporting partnership in mental

POLICY TITLE	**RECORDS MANAGEMENT POLICY**
POLICY REFERENCE	COR2
POLICY CATEGORY	Corporate
RELEVANT TO	All Care Trust Staff.
DATE PUBLISHED	Sept 2006
IMPLEMENTATION DATE	Sept 2006
DATE LAST REVIEWED	Nov 2006 (Mar 07)
NEXT REVIEW DATE	February 2008
RESPONSIBLE PERSON	Timothy d'Estrube, Information Governance Manager
CONTACT DETAILS	Email: timothy.d'estrube@candi.nhs.uk | Telephone: 020 7530 3019
ACCOUNTABLE DIRECTOR	Claire Johnston, Director of Nursing and Performance Signature and date
APPROVED BY	Records Management Group Date: 31/08/06 (Ver 1.3)
APPROVED BY	Risk and Assurance Committee Date: 21/02/06 (Ver 1) | Information and ICT Strategy Group Date: Insert Date (Ver 1.3)
APPROVED BY	Clinical Governance Committee Date: 11/07/06 (Ver 1.1)

DOCUMENT HISTORY

Date	Version	Amendments
Feb 2006	1	New policy
Jun 2006	1.1	Inclusion of section 5.8.5
July 2006	1.2	Inclusion of sections 5.1.4, 5.9 and 5.10
Aug 2006	1.3	Inclusion of section 5.12
Mar 2006	1.4	Amendments to 5.8.4, 5.9, 5.10, Inclusion of 5.9.3

MEMBERSHIP OF THE POLICY DEVELOPMENT/ REVIEW TEAM	Alison Chapman, Clinical Governance Facilitator Ian Diley, Clinical Governance Facilitator Timothy d'Estrubé, Information Governance Manager (Records Manager)
CONSULTATION	Information Manager Clinical Governance Department Records Management Group

DO NOT AMEND THIS DOCUMENT

Further copies of this document can be found on the Care Trust intranet.

CONTENTS

1 INTRODUCTION/BACKGROUND

This policy has been created in order to provide a framework and guidance for Care Trust staff to manage the requirements and processes involved with creating, keeping and managing clinical and corporate records.

The policy was developed after a literature review and analysis done by the development group (membership above). The first drafts will be circulated amongst the development group for a first revision. The agreed draft policy is to be then approved by the Care Trust Board.

This policy has been introduced to ensure that clinical and corporate staff can create, maintain and use records and information within defined standards for the Care Trust. In following the concepts of this policy staff will be able to efficiently and effectively create and manage records and information.

All staff (where applicable) are required to abide by existing legal and appropriate organisational, and professional guidance as below:

- Camden and Islington Mental Health and Social Care Trust – Code of Confidentiality For Sharing Client Information Within Community Mental Health Teams, August 2001.
- Camden and Islington Mental Health and Social Care Trust Access to Care Records Policy 2005.
- Data Protection Act 1998 and Freedom of Information Act 2000.
- Nursing and Midwifery Council Guidelines for Records and Record Keeping, January 2005.
- London Borough of Camden Social Services Good Practice in Record Keeping - Social Services Standards
- London Borough of Camden Social Services Access to User Records Policy & Practice Guidance
- London Borough of Camden Social Services File Retention Policy
- Camden and Islington Area Mental Health Committee Protocol for Multi-Agency Information Exchange, July 2000.
- Camden and Islington Mental Health and Social Care Trust - Care Programme Approach Operational Policy, April 2001
- Clinical Negligence Scheme for Trusts - Mental Health and Learning Disability Clinical Risk Management Standards, NHS Litigation Authority, June 2005.

2 AIMS OF POLICY

This policy provides standards against which the Care Trust can create, maintain and dispose of records and information against best practice.

3 OBJECTIVES/SUMMARY OF POLICY

This policy is intended to:

- provide overarching standards for Records Management within the Care Trust;
- provide guidance to staff in the creation, use and disposal of Care Trust information and records;
- standardise formats of general documents.

4 POLICY SCOPE

This policy is intended only to provide standards for general concepts within Records Management. **It is not intended to be a guidance manual for front-line staff**, rather this is the overarching policy to which other local or subject specific policies are responsible. This policy is specific to Records Management issues relating to the creation, development, maintenance and disposal of electronic and manual documents. This policy does not specifically deal with the following issues:

- Data Protection, Freedom of Information and Confidentiality
  Please see the following Camden and Islington Mental Health and Social Care Trust documents for further information: Access to Care Records Policy, Access to Personal Records for Research Purposes Policy, Access to Information Policy, Code of Confidentiality.
- Use of Emails
  Please see the following Camden and Islington Mental Health and Social Care Trust documents for further information: Internet and Email Policy.

For other issues or help please contact the Care Trust's Records Manager or Clinical Governance Department. This policy, and any of the above-mentioned policies are available from the Information Governance Manager, your line manager or the Care Trust's Intranet Document Store.

5 GUIDELINES AND POLICY STATEMENTS

5.1 Forewords and Descriptions

This document uses a number of terms. These are defined here.

5.1.1 Definition of "Records Closure"

The term closure in reference to records or information either refers to the sealing of a record from having any new entries made within or that the information held within officially ceases to be valid.

5.1.2 Definition of "Documents"

The term "document" for the purpose of this policy refers to any type of record or set of information held by the Care Trust. This includes all manual records and electronic files of any kind. Example of documents includes, but are not limited too:

- administrative records (including personnel, estates, financial and accounting, litigation, complaints files);
- Any medical or care register;
- patient care records;
- any test results including x-rays and other imaging information;
- audio and visual records of any kind;
- photographs, slides and other images;
- any communications, including letters, e-mails, web-pages, telephone texts.

Documents can be stored in any medium including but not limited to:

- paper;
- computer hard drives, CD-ROMs, floppy disks, RAIDs, flash memory (USB devices)
  In any kind of format, including but not limited to: Microsoft Office documents, PDFs, AASCII, etc;
- microfiche, film or tape;

- as part of or comprising of a database or spreadsheet.

5.1.3 Definition of "Case Notes"

For the purpose of this document the term "Case Note" refers to the collection of documents that comprise the case history of a service user for a particular service or set of services. In all cases this is a specifically organised and bound collection of documents enclosed in a protective cover of some sort, or is a specifically organised set of electronic documents that exists in a filing system or as part of a database.

5.1.4 Definition of "Continuous Integrated Multidisciplinary Case Notes"

A continuous integrated multidisciplinary case note (C.I.M. case notes for short) is fully explained in section 5.8.5. As a brief description it is the section of case notes where care professionals record their observations and progress notes. There is a particular methodology associated with C.I.M. case notes, as explained in section 5.8.5.

5.2 How to Use this Policy

This policy is intended as an overarching policy for Records Management within the Care Trust leaving it flexible to encompass all records and information types. This policy is intended to have a chain of sub-policies beneath it, narrowing in focus but becoming more detailed, culminating in a local process or procedure document.

This is not a policy for front line staff usage. This policy is the policy against which the Care Trust's Records Management function sets its general standards and the framework in which it operates.

For Records Management guidance on specific issues please consult the relevant sub-policy or contact the Care Trust's Records Manager, Information Governance Manager or Clinical Governance Department, all of which are based at Care Trust headquarters, 2nd floor East Wing, St Pancras Hospital.

5.3 Responsibilities within the Care Trust

This section outlines the responsibilities for Records Management at the various levels of the Care Trust.

5.3.1 Responsibility for the Policy at Board Level

The Care Trust's Board has overall responsibility for the well-being of the Care Trust's records and information. Asides from those responsibilities similar to Records Management under Data Protection and Freedom of Information Legislation, the Care Trust Board has responsibilities to ensure that:

- Care Trust staff have a safe and secure work environment for undertaking Records Management;
- Care Trust staff have appropriate support, guidance and training for Records Management activities;
- information held by the Care Trust is kept safely and securely until it is removed or destruction;
- information held by the Care Trust is made available for appropriately clinical and corporate use.

5.3.2 Chief Executive Responsibility

The Chief Executive is empowered by the Care Trust Board to fulfil the duties of the Care Trust's Records Management Responsibilities. Additionally the Chief Executive will ensure that:

- Records Management is performance managed throughout the Care Trust, in all directorates, services and departments;
- Records Management receives sufficient resources to enable staff to meet the Care Trust's performance targets.

5.3.3 Directors Responsibility

All Directors will ensure that:

- all their services and department comply with Records Management standards;
- all of their services and departments are adequately resources such that they can meet records management targets.
- all of their services and departments are adequately resourced such that they have safe and secure storage for documents and staff.

5.3.4 Director Responsible for Records Management

The Executive Director responsible for Records Management is empowered by the Chief Executive to fulfil the duties of:

- preparing the strategy for Records Management within the Care Trust;
- implementing the performance monitoring of Records Management within the Care Trust. In doing so the Executive Director will provide the Executive Board with suitable information for performance management on a routine basis as requested by the Chief Executive;
- as appropriate, the Executive Director is responsible for, or the sponsor of, the budgets and contracts for Records Management functions;
- being the chair of the Records Management Committee;
- setting the objectives, in conjunction with other relevant authorities, of the Care Trust's Records Manager.

5.3.5 Senior Management Responsibility

All Senior Managers will:

- take appropriate and effective action to ensure records management standards are met within their services and departments;
- ensure that appropriate Records Management issues and incidents are reported via the Care Trust's incident reporting procedure.

5.3.6 Records Manager

The Care Trust's Records Manager is empowered by the Director responsible for Records Management to hold corporate and strategic responsibility for Records Management within the Care Trust. In terms of physical records this includes:

- all aspects of storage, archiving and transportation of records;
- protocols and processes for accessing Care Trust records;
- the process and protocols of creating, maintaining and destroying records
- authorisation for the destruction or permanent preservation of records;
- the schema used to identify and archive records;
- the inventory and tracking systems for the storage, archiving and transportation of records.

In terms of electronic records this includes:

- directing appropriate system managers to include the needs of Records Management into their system's strategy;
- designing and implementing appropriate systems to support Records Management.

The Records Manager is further responsible to ensure that, with support from appropriate parties, all the systems and processes support the Care Trust's requirements of Data Protection and Freedom of Information.

5.3.7 Responsibilities of the Data Protection Officer

The Care Trust's Data Protection Officer is responsible for:

- ensuring, with other relevant parties, that data / information exchanges in relation to this policy are compliant with the Data Protection Act 1998;
- ensuring that processes for information under the Data Protection Act 1998 are compliant with this policy.

5.3.8 Responsibilities of IT and Care Trust Clinical Systems Departments

Information Technology and Systems departments are responsible for:

- working with the Records Manager to meet the Care Trust's Records Management Strategy;
- ensuring that the systems and network they are responsible for are adequately supporting or working towards supporting Records Management within the Care Trust;
- providing appropriate monitoring information for the performance management of Records Management.

5.3.9 All Employees of the Care Trust

All Care Trust staff are expected to:

- meet the Records Management requirements relevant to them;
- feed back issues through their line management whenever this policy is in conflict with professional values, legal or statutory obligations and/or is generally impractical;
- ensure their actions and decisions are based on the guidance and best practice of the Care Trust and when in doubt to seek appropriate guidance and support through their line management or other appropriate identified individuals.

5.4 Third Parties

The Care Trust may employ or empower third parties to assist or otherwise be involved with Care Trust documents. The following therefore relates to any instance of third party interaction with Care Trust Documents.

5.4.1 Empowering Third Parties

All third parties involved with Care Trust documents must be empowered to do so. The empowerment must be given in writing and must be signed by the Care Trust's Records Manager or a member of the Care Trust Executive.

5.4.2 Conditions of Third Party Empowerment

Any instance of the Care Trust empowering a third party must be under the following conditions:

- the Third Parties must sign a confidentiality agreement to protect the Care Trust's information. This agreement must include an indemnity clause. Alternatively the Care Trust may accept the existing confidentiality safeguards of the 3rd party. When in doubt

about 3rd party's confidentiality arrangements the Care Trust's Caldicott Guardian, Data Protection Officer or an Executive Director should be consulted. The Caldicott Guardian has final decision on the acceptance of third party confidentiality arrangements.

- the Care Trust prior to providing empowerment must confirm that the third party can fulfil any confidentiality agreements/arrangements;
- third parties must be given defined access rights to Care Trust information, documented within the confidentiality agreement.

5.5 Archived vs Active Documents

This policy applies only to Active Documents; documents that are currently being created and used. Documents that have been archived prior to the implementation of this policy need not be retrospectively made compliant. Archived Documents that come out of the Archive and into use again, particularly Case Notes, must be made compliant.

5.6 Standards for All Documents

The Care Trust requires minimum standards to be met in order for documents to remain identifiable and useful when archiving, particularly after significant time has elapsed after their closure.

5.6.1 Identification Standard for All Types of Documents

All Care Trust documents, electronic or otherwise, will carry some identification that they belong to and/or were created by the Care Trust. Documents including, but not limited to:

- meeting minutes of any meeting, group or committee;
- external correspondence of any kind;
- briefing papers, proposals, project plans, policies reports;
- any material for public consumption.

Must carry the Care Trust logo on at least the front page of the document. Where appropriate, the Care Trust logo or similar identification should be present on other parts of the document, particularly if sections of the document can be used separately from the main. Where appropriate it would also be good practice to include in headers or footers of the document the:

- number of pages and the page number;
- author of the document, including the department or service of the author;
- name of the document;
- date of creation or publication.

Documents including, but not limited to:

- daily care records, care related observations and contact notes or any other material within the Case Notes;
- published database printouts or reports, spreadsheets.

Must identify somewhere on the document that the document was created by the Care Trust, and as appropriate, from which ward, service or site the document came. For documents that can be separated into components, every component or sheet needs to bear the identification. This is particularly relevant to case notes.

5.6.2 *The Use of Signatures on all Types of Documents*

Signatures are an important part of any record, clinical or corporate. The following applies to any signature made on any type of record:

- all signatures must be accompanied by a plain text description of the signature;
- documents that require a signature (i.e. significant legal, commercial or medical documents) must have a signature signed in black pen. It is not acceptable to provide an electronically scanned signature or provide the name in type for significant documents. Electronically scanned signatures do not currently carry the weight of evidence and therefore cannot be used in significant documents;
- all signatures should be written in pen, and all signatures in case notes must be written in black pen

The Care Trust will keep a record of all signatures of all applicable staff in line with the requirements of CNST. For further information please see the CNST Standard for Mental Health, Standard 4.

5.6.3 *Use of the Care Trust Seal*

Only certain documents require the Care Trust seal. Descriptions of those documents and the use of the Care Trust's official seal can be found in the Care Trust's Standing Order Policy. In general the seal must be affixed to building, engineering, property or capital documents.

5.6.4 *Standards for Meeting Minutes and Agendas*

All official meeting minutes and official agendas, regardless of the type of meeting, need to include on the front page the following information:

- name of the group meeting;
- date, time and for agendas only; place of meeting;
- chair of the meeting;
- meeting's members, and meeting attendees/observers (for meeting minutes only). Members are permanent members of the group, attendees are visitors or observers to the group;
- contact person, service or directorate from where further meeting minutes and reports could be received;
- the date, time and place of the next meeting.

5.6.5 *Standards for Corporate Documents*

All corporate documents, for example meeting minutes, proposals, reports, committee papers, must include the following in every relevant section of the document:

- author(s)/creator(s), be it a specific person, service or directorate;
- contact details of the author(s)/creator(s);
- date of creation or publication of the document;
- source of any data used, and the date the data was collected.

If known and applicable, the date the document becomes invalid or the conditions under which the document becomes invalid.

5.7 Contractual Considerations of Records

The Care Trust, when engaged with supplying and buying services with other organisations, must consider the ownership of the records and information created in supplying the service.

All SLA's or Service provision contracts must explicitly state the ownership of any resulting records or information produced under that agreement.

As a general rule, the Care Trust shall seek to own records and information resulting from services it bought, and shall seek to divest to the purchasing party records and information resulting from providing services.

5.8 General Standards for Clinical Documents

These standards have been introduced to ensure that clinical staff have access to all the information they need about the service users for whom they care. Serious and local incident reviews have often highlighted the inadequacies in Care Trust systems for accessing and maintaining service user specific information. These record keeping standards are a practical response to these issues and should be used by all members of the multidisciplinary team. These standards should be read in conjunction with standards for CPA and Risk Assessment documentation and local standards for care planning and auditing.

This section outlines general standards specifically for clinical documents. These standards are not intended for documents that are corporate documents.

5.8.1 Definition and Purpose of a Case Note

Case notes are intended to facilitate the care and treatment received by a service user and to demonstrate that such care is offered in an accountable and appropriately sensitive manner. Case notes exist as either a set of organised and bound documents or as an organised set of electronic information.

Case notes must enable:

- clear communication. An authorised person will, by reading the notes, be able to immediately identify a service user's current needs and care plan;
- the clear recording of the care provided;
- exercises in evaluating the care provided.

Case notes are:

- confidential;
- potential legal documents;
- potential evidential documents;
- accessible to service users and legally empowered organisations.

Case Notes need to be:

- accurate;
- non judgmental;
- contemporaneous;
- objective;
- factual;
- comprehensible;
- up to date;
- signed with a full signature with name and designation clearly printed for every entry on every page;
- accurately dated.

5.8.2 Identification Standard for Case Notes

For each service user the Maracis number will uniquely identify all case notes that are Care Trust property. All services, regardless of Maracis usage, assign the case notes to the corresponding Maracis number of the service use.

Case note folders will be assigned volume numbers for each service. Volume numbers increment additionally, with the first set of case notes being considered Volume 1, the second Volume 2, etc.

All case notes must have the Maracis number, the patient name and the volume number clearly identifiable on the front cover.

Should the front cover be damaged so that any of the above mentioned identifiers are illegible, requires the case notes folder to be replaced.

Case notes can have additional identifiers on the front cover, such as other system numbers like the Maracis number (e.g.: SWIFT, Framework-I or NHS number)

5.8.3 Physical Standards for Manual Case Notes

Care Trust case notes will comply with the following characteristics:

- *Be manageable in size and weight*
  All case notes should be of a width that they can be gripped easily.

- *Durable*
  Case notes must be bound in such a way that when closed they can suffer the spillage of liquid, jabs with pens and pencils, dragging across surfaces, stacking at awkward angles, being bumped, crushed, dropped and any other general mistreatment of the type that can be found in an office or clinical environment with minimal or no damage to the information contained within or the identifying marks on their covers.
- *Be bound so that loss of documents is minimised*
  All case notes must demonstrate that they can be held upside-down and shaken without the loss of documents.
- *Contain clear instructions regarding filing*
  All case notes must have a set of instructions that are legible and outline the use of each different sections of the binder.
- *Be arranged so that the current Care plan/CPA/Risk Assessment is readily identifiable.*
- *Be arranged so that Mental Health Act/legal documentation is readily identifiable.*
- *Be arranged so that machine produced recordings can be securely stored.*
- *Contain a designated place for the recording of hypersensitivity reactions and other information relevant to professionals involved in the care of the service user.*

5.8.4 Making an Entry in Manual Case Notes

The Following Standards are based on the NMC Guidelines for Records and Record Keeping (2002) and NHSLA, Clinical Negligence Scheme for Trusts – Mental Health and Learning Disability, Clinical Risk Management Standards, June 2005, and amended in light of local recommendations.

Entries into any case note must:

- *Be factual, consistent and accurate, avoiding subjective statements wherever possible.*
  Professional opinions, judgements and speculations are acceptable to record. However in recording such information authors must ensure that they have done so in a professional style of writing and have not used subjective or disrespectful language. Where it is not otherwise obvious authors **must** include justification for their statements and **must**,

particularly in the relation to professional speculation, indicate their statements to be something other than an observation.

- *Be accurately timed and dated at the commencement of the entry*.
- *Be signed and the name and designation of the staff member printed at the end of the entry; self-inking pads may be used.*
- *Be written continuously, with no intervening gaps between records. In the event of any gap between one entry and the next, and where a line is incomplete at the end of an entry, the gap should be struck through.*
  This does not mean that entries must be devoid of paragraph breaks and normal text spacing. Entries must be made as legible as possible, which includes allowing paragraph breaks and a space between entries. However what must not happen is that there is the ability to add, correct or change an entry. Every space that is created must have a line or other indication made in that open space which prevents subsequent changes to the original entry.

- *Be written legibly in black ink.*
- *Not include jargon, meaningless phrases, irrelevant speculation or offensive comments.*
- *Avoid abbreviations (except where these are in widespread clinical or general usage).*
- *A qualified member of staff must countersign all pre-registration student nursing staff entries.*
- *Efficiently recorded, being concise and minimising duplicate entries.*

- ***All records of contact with service users should be contemporaneous, that is completed within one working day of the contact occurring.***

- ***Unless securely stapled together, every page within the case notes must identify the service user, and if not written elsewhere, by including the service user's name and Maracis number at the top left corner.***

- ***All Documents and entries in case notes must be directly relevant to the care being provided***
  Under no circumstance should non-clinically relevant information be included in a case note binder. Unless certified as clinically relevant by a care professional, the following documents must not be part of a case note. This includes, but is not limited to:
  - complaints files;
  - court or legal documents relating to grievances;
  - administrative records.

  Where it is not obvious that a document is clinically relevant, a description of why the document has been included as part of the case notes must be included.

5.8.5 Requirement of Continuous Integrated Multidisciplinary Notes

All case notes created within the Care Trust should be written so that they form a single continuous chronological history of care provided by all care workers within a particular Care Trust service. This means that all health and social care professionals within a service will contribute to the same set of case notes, literally using the same pages within the same section of the case notes folder to record their progress / continuation / observation notes. Entries in these notes will be chronological, and are written following on from previous entries. For instance, if an Occupational Therapist or Art Therapist, Social Worker, then Consultant saw a patient in chronological order, the OT/AT would write their entry at the top of the page, the Social Worker makes their entry below the OT/AT and the Consultant below the Social Worker.
Health and Social Care professionals contributing to the case notes in this way may only do so if they are employed as part of the service the case notes belong to and they are otherwise required to follow Care Trust policies and procedures.

Case notes written according to this methodology will be referred to as:

- *Continuous* (because the entries make a continuous history of care when read)
- *Integrated* (because the entries of all different health and social care professions and occupations of the care service are included into a single section of a single case notes folder)
- *Multidisciplinary* (because the method of entry deliberately facilitates working in a multidisciplinary team)

The acronym referring to this methodology of creating case notes will be C.I.M. Case Notes.

5.8.6 Making Alterations and Additions to Case Note Entries

Corrections of entries in case notes must be obvious but ensure that the original entry is not made illegible. Where appropriate all records to be corrected should have a single line striking them out, so that the original entry is still readable. No 'Tippex' or other correction pens should ever be used.

Where a correction or addition is to be inserted the correction or addition must be made legibly. If the new entry cannot be made on the same page as the original then an additional page must be placed adjacent to the original page. An indication of where the correction or addition is to be found must be written legibly and adjacent on the same page as the original entry.

All alterations and additions must be dated, timed and signed.

5.8.7 Standards of Paper for Case Notes

Case Notes must comprised of the following types of media:

- papers and inks that are coloured in such a way that they can be photocopied accurately and without the loss of any detail;
- papers that are robust and can withstand regular and repeated use within the binders without tearing. Regular white multi-purpose type paper is preferred. Under no circumstance should the type of paper found as rolls for fax machines be included in case notes. Where information is sent by fax or stored on flimsy paper or using inks that tend to fade, the information must be photocopied. Photocopies of original but unsuitable records must be signed and dated by the photocopier.

5.9 Sealed Information

In some circumstances information may be deemed as confidential within the case note. In order to protect this information it is appropriate to place the information within a "sealed" envelope.

5.9.1 When it is appropriate to offer Sealed Envelopes

Sealed envelopes are intended to keep information that a service user has extraordinary reservations about recording or providing to the Care Trust. Only in the case where the service user would otherwise be reluctant to engage with Care Trust services or they have made a direct request for information to be removed or withheld from sharing with any other services or other care workers should a sealed envelope be offered as an option. A good example could be information relating to the service user's sexual health, which was disclosed to a single therapist and in itself has no direct importance to care provided by other services or care workers.
Sealed envelopes must not be used when for information that is pertinent to the safety of the service user or care workers. For instance a suicide note intended for the future should not be placed into a sealed envelope. It remains the decision of the care worker(s) as to what information can or cannot be placed into a sealed envelop. Care workers can contact the Data Protection Officer for guidance and advice when creating a sealed envelope.

5.9.2 Creating a Sealed Envelope

As there is an element of risk involved with creating a sealed envelope, consent from the service user or information supplier to make this information generally unavailable must be obtained. In obtaining consent Care Trust staff must explain the risks involved of not having this information available to other staff and corporate processes. The explanation must also include a description of situations when the sealed envelope may be opened without the consent of the service user/information supplier. Staff are well advised to include a letter of consent signed by the service user/information supplier to indicate their agreement for the sealing of their information. Any consent letter can be stored inside a sealed envelope, however for audit purposes an indication of consent should be available without having to open the envelope (Signing by the service user/information supplier of the envelope itself is sufficient).

A sealed envelope should be a regular envelope with sufficient volume (using multiple envelopes if necessary) to contain the appropriate case notes. The envelope should be hole punched in line with the holes punched in the case notes. The envelope should not be so large as to disrupt the regular filing of the case notes and should not be so large as to exceed the dimensions of the case note folder.

The sealed envelope should contain a sufficient description on its cover so that the information contained within can be identified without revealing the sensitive contents. The description should also indicate when it is appropriate to open the envelope (e.g.: In the event of a particular emergency or after a certain date). Also required are the name of the care worker who was responsible for sealing the information, the signature of the service user or information provider (if appropriate) and the date the information was sealed.

When inserting a sealed envelope it is most appropriate to place the envelope at the back of the Continuous Integrated Multidisciplinary case notes section, however if this makes the case notes difficult to read then it can be placed at the very back of the case notes. If placing at the back of the case notes a notice must be placed within the Continuous Integrated Multidisciplinary case notes section to ensure that care workers are alerted to the presence of the sealed envelope.

The sealed envelope should be inserted into the case notes so that the envelope and the case notes are both bound.

5.9.3 Opening a Sealed Envelope

Opening a sealed envelope should only be done when there is a direct clinical or corporate need to retrieve the information. Unless otherwise impractical in an emergency situation, those staff interested in opening a sealed envelope should contact the service user or information supplier who agreed to seal the information, or if this is not appropriate, the staff member who created the sealed envelope to obtain approval to retrieve the information. If neither the staff member nor the service user/information supplier is available then the Caldicott Guardian or the Data Protection Officer should be consulted.
When opening a sealed envelope, the following must be recorded in the service user's care records:

- The justification for the decision to open the envelope
- The date the information was retrieved
- The name and clinical/corporate functionality of the person(s) retrieving the information

The following actions must be taken once information is retrieved from a sealed envelope:

- Notice must be sent to the Caldicott Guardian and Data Protection Officer
- If appropriate, a reasonable effort must be made to contact the service user/information supplier and inform them that the information was retrieved
- If appropriate, once the use of the information is completed, the information should be re-sealed. The new sealed envelope should indicate the original staff member(s) and the new staff member who sealed the information

Note that staff who originally agreed with the service user/information supplier to created a sealed envelope may access the sealed information normally to carry out their clinical/corporate responsibilities without having to carry out the above instructions.

5.10 Creating and Protecting Case Notes of Employees or other notable people

There are occasions where care is provided to people known by name to Care Trust staff. In most cases this will be employees (or ex-employees) of the Care Trust and high profile members of the public. It may also include family members or friends of Care Trust staff. In these situations it may be appropriate to disguise the identity of these service users' case notes (both electronic and paper-based) in order to prevent extra-Trust and intra-Trust breaches of confidentiality.
Notes should only be altered in such a way as to make them difficult to casually locate. The interior records of the notes should never be altered for disguise.

The following section only applies to case notes, and not Human Resources or Occupational Health or any other type of record.

5.10.1 Considerations for Identity Disguising

Any disguising of a case note's identity can potentially complicate the provision of care, and can in some cases be risky to the health and safety of the service user and Care Trust staff. Therefore, methods of disguise should only be employed where the risk of not being able to immediately locate and use service user information is outweighed by the potential damage to the service user should it be discovered that they are receiving care.

As there is an element of risk involved with disguising a care records identity, consent from the service user or information supplier to make their care information difficult to locate must be obtained. In obtaining consent Care Trust staff must explain the risks involved of not having this information available to other staff and corporate processes, particularly for emergency situations, and that the responsibilities for this risk is carried jointly between the Trust and the service user. Staff are well advised to include a letter of consent signed by the service user/information supplier to indicate their agreement for the disguising of their information.

Service users publicly known to be receiving care could be offered a disguise to the identity of their case notes if they would otherwise refuse to have case notes created or are uncomfortable at having identifying information held in a particular medium (e.g. held electronically). The decision to offer disguised case notes would have to be taken by the responsible care worker for that service.

Disguising the identity of the service user should not automatically be considered if the service user is publicly known to be receiving care. Staff are already under confidentiality agreements that forbid them from looking at case notes with which they do not have a legitimate relationship.

5.10.2 Principles of disguising case notes

There are a number of general principles that must be adhered to when disguising the identity of a case note.

- The disguise should only affect the ability to locate the particular case notes, and should not affect the ability of the case notes to be read or used.
- The disguise should not disrupt or damage the general system of locating records of that type. As examples, electronic files should not be named in such a way as they become unreadable by the system, and a paper file should not have a false Maracis number on its cover.

- If possible, the information required for receiving payment for the services provided should not be removed. For instance, the NHS number of the service user if it is required to be part of the person's identity for the purpose of billing should remain as part of the identifying information of the case note.
- Only human-readable information should be altered. Machine-readable information, such as the Maracis number or NHS number, need not be removed or altered because it is already meaningless to the casual observer.

5.10.3 Example methods of disguising case notes

The following are examples of how case notes can be disguised. Please note that any disguising of case notes must be explained to the service user, and must receive agreement from the service user that they accept the risks of not being able to locate case notes. Please remember that records may be required in an emergency by another organisation, or by people within the Care Trust that do not otherwise have knowledge about the method of disguise.

- *Changing the name*

  Service users' names can be changed quite easily. On a gradient of risk, it is better to change one or two letters of a name rather than to substitute an entirely different name. For instance "Crystal" could become "Kristal" or "James" could be shortened to "Jim" (or vice versa). Middle names or maiden names could also be used.
- *Using initials*

  It is acceptable to use the initials of the service user
- *Using Alias*

  The use of aliases should be avoided unless it is unlikely that the service user would ever require emergency care.

The postcode is often a key piece of information. If changes are made to the address of a service user it is important that the postcode remains unaltered. As a minimum, the postal prefix should always be kept, rather than dropping the entire postcode.

5.10.4 Sealing Employee Information

Employee case notes are particularly difficult if the information is inappropriate to disclose to the employee. Where there is a risk that the employee could through regular working arrangements receive the inappropriate information (e.g. via Maracis), special precautions should be taken to prevent casual access.

In most cases the danger will exist on an electronic system. Where the electronic system cannot specifically block access to the employee's files, the care team should consider making a special note within the system that such inappropriate information can only be found in the paper-based files. This decision should be weighed against the potential risk of not having this information available online.

Where the inappropriate information is kept in paper records, consideration should be made to place the information into a sealed envelope (See Section 5.9).

5.11 Transportation of Records

Care Trust records, clinical or otherwise, must be transferred in a secure and safe manner. The following section outlines the requirements for transportation of Care Trust records.

5.11.1 Safety and Security

All transportation of Care Trust records must be done in a safe and secure manner. Most methods of transport available to the Care Trust are acceptable for non-confidential and non-important documents.

Confidential and important documents however must be transported by approved methods that ensure minimal risk of loss or delay. Transportation requirements differ depending on the method of transportation or communication, however all approved methods must have the following characteristics:

- have confirmed and documented senders and recipients;
- have specific addresses or locations indicating where the records are being sent;
- have a period of time confirmed by the sender and receiver in which the records/information is expected to arrive.

The Records Manager, apart from the methods deemed acceptable in this policy, has sole discretion on certifying a method of transport as being acceptable for use within the Care Trust.

5.11.2 Transportation of Original Documents

The transportation of original records, particularly those of high importance and are unique, (e.g.: Care Records), should be avoided whenever possible.

Copies of documents should be made and provided instead of originals, particularly if the document is be transported to locations outside of the Care Trust or will be absent from its "home" location for a significant period of time.

5.11.3 Acceptable Transportation of Physical Records

In order for a method of transporting physical records to be acceptable for approval it must have the following characteristics:

- have confirmed and documented pick-up and delivery dates and times;
- are not left unattended or unprotected at any point.

5.11.4 Acceptable Transport of Information over a Network

In order for a method of transporting electronic records over a network to be acceptable for approval it must have the following characteristics:

- the information has suitable encryption and password protection;
- the receiving address or network must not be publicly accessible, unless the request for information specifically requires the information to be sent to such a network (for instance, no information should be sent to email addresses ending in hotmail.com or yahoo.com unless it is specifically required).

See the Care Trust's Internet and Email Policy for further information.

5.11.5 Acceptable Transport of Information via fax machines

Records and information transported by fax machines must be:

- transported via "safe haven" faxes (As per Caldicott Guardian Guidance) or equivalent unless it is required otherwise by the request for the information;
- must be confirmed upon receipt.

See the Care Trust's Safe Haven Policy for further information.

5.11.6 Transport of Information/Records Outside the Care Trust

The Care Trust's Caldicott Guardian, Records Manager or Data Protection Officer must approve any flow of documents outside of the Care Trust to another organisation that is an ongoing arrangement to provide information and is not considered a unique and singular event.

Any ongoing, routine provision of information must be provided within a Subject Specific Information Sharing Agreement or their equivalent (as per Care Trust's policies and protocols on Information Sharing), or under the written instruction of the Care Trust's Caldicott Guardian.

Singular events of transferring information must be approved by the Care Trust's Caldicott Guardian or Data Protection Officer.

See the Care Trust Information Sharing Protocols for further information.

Please note that routine discussions with 3rd parties involving confidential information must be done within the framework of a Data Sharing Protocol. Where protocols are not yet implemented the Caldicott Guardian should be consulted for conditional and temporary authorisation while a protocol is being put into place.

5.11.7 Acceptable Methods of Transport

The following methods of transport are considered acceptable:

Transport of physical files:

- delivery by hand by a Care Trust employee (under the proviso that they do not leave the records unattended or unprotected at any point);
- Royal Mail Recorded Delivery;
- commercial courier companies on the approved list (contact Transport Manager, St Pancras Hospital for details).

Transport on electronic networks:

- emailing to a "CANDI" email or FTPing within the "CANDI" network.

Transporting via fax machines:

- faxing to any of the Care Trust's listed "Safe Haven" faxes.

5.11.8 Restrictions on taking Records Home, on Assignment and Hand Delivery

Care Trust staff personally transporting records must do so during regular working hours (for the staff member) and while en-route, be engaged entirely with Care Trust business. Staff members engaging in personal business while transporting records invalidate the Care Trust's insurance. For this reason staff must not carry notes with them on non-work business.

Staff who are providing Care Trust services or on Care Trust business that requires them to be away from the Care Trust for multiple days will be considered on Care Trust business for the entirety of their assignment. Care Trust records should be returned within one working day of their assignment finishing and their return to the proximity of London. Where necessary, the Care Trust will accept the costs and delivery of records via register mail or courier if staff members cannot reasonably be expected to return the records in time. Authorisation for the use of couriers/registered mail in these situations must be authorised by the Records Manager or the staff's line manager prior to the engagement of the service. Staff will be responsible for the safety of the records the entire time they are with them on assignment.

When hand delivering records staff must not leave the records unattended or unprotected at any time. If records are being transported in a vehicle and the vehicle must be left unattended while performing some other Care Trust business, the records must be out of sight and the

vehicle secure from entry. It is not appropriate to leave records unattended in bicycles or motorbikes.
Only in the most exceptional circumstance should Care Trust staff take service user records/information home.

In any instances where service user's records/information are taken home by a staff member they must first seek permission from their immediate line manager, or the Service Manager on call. Staff taking service user records/information home must ensure the records/information remain safe and secure throughout their absence from the Care Trust. Records/Information must be returned to the Care Trust as soon as possible. Staff members taking records/information home must, in addition to sign-out procedures for the particularly library the records/information is from, leave 24 hour contact details as to where they can be contacted if the records are urgently needed.

All records/information, once their immediate use is finished, must be returned to the Care Trust within one working day.

5.11.9 Tracking Systems

Where appropriate the Care Trust shall implement tracking systems for the movement of confidential and/or sensitive information. At minimum these tracking systems will include:

- the item's corporate reference identifier, Maracis Number of a service user, or other identifier;
- a description of the item;
- the person, service or department to who is sending the item;
- the person, service or department to whom the item is being sent;
- the date of the transfer.

5.12 What to do when records are lost or stolen

Care Trust records are important and valuable sources of information, be they care records or corporate records, electronic or paper. The loss or theft of this information can seriously compromise the provision of care or cripple corporate projects or decision-making. Any loss or theft of Care Trust records must be reported via an incident report form (IR-1 form).

5.12.1 Good business practice to prevent records loss or theft

The Care Trust assumes that all records are secured appropriately from loss or theft. As loss or theft is not completely preventable however, there are a number of actions services can take beforehand to ensure that any loss or theft of records is detected and contained quickly. The following best practice is recommended for all services and functions:

- Keep every record storage area tidy. In this way it is much easier to locate files and hence know if files are missing.
- When records are being transported, keep an inventory of which records they are and ensure that both the sending and receiving parties have copies. Ensure that the receiving party confirms the receipt of each record.
- Don't keep records you don't need. Destroying old records means that they cannot be lost or stolen, sending them to long-term storage means that they are safely out of the way.
- Be sure to communicate with the receiving party when they should expect to receive records that you are sending.
- Keep records out of sight. Particularly if you are not using records, make sure that they are put away out of sight to prevent casual theft.

5.12.2 What to do when records are stolen

Where Care Trust staff suspect or know that records have been stolen they should do the following as soon as possible:

- Report the incident to their line manager.
- Inventory the records that are missing.
- Inform the police, particularly if they are care records (Managers may be the best person to do so if the situation is no longer urgent).
- Ensure that any remaining records are not vulnerable to the same situation of theft. Records should be moved to a more secure area.
- Complete an IR-1 form to report the incident.
- Where not already documented in the IR-1 form, document the details of the theft, including:
    - All actions taken
    - How the theft was discovered and/or carried out (if known)
    - Descriptions of the information taken
- Secure any video surveillance, security logs of any devices (including door codes and server access records), sign in/sign out logs, and if applicable any physical evidence. When retrieving such items ensure that the process used to secure them does not corrupt or taint them (e.g.: Avoid getting your fingerprint on them). When in doubt consult with the appropriate authorities or line manager.

All documentation and evidence collected should be provided to staffs' line management for safekeeping as soon as possible.

5.12.3 What to do when records are missing

Where Care Trust staff suspect or know that records have gone missing they should do the following as soon as possible:

- Inform their line manager.
- Inventory the records that are missing.
- Document when the records where last seen and what they were last used for.
- Document any actions taken to search for the records. Records should be searched for via a coordinated search plan (see below).
- Complete an IR-1 form to report the incident.

5.12.4 Creating and using a Coordinated Search Plan

All Care Trust services and sites should prepare a coordinated search plan for the event of records going missing. This plan will be used to coordinate a search pattern and ensure that all relevant areas are accounted for during any search.
The Coordinated Search Plan will be different for each site and service as it depends on the layout and business of the area. The plans should take into account high-risk areas first, followed by the most relevant areas the records could be. As such the sequence of a search plan should be in order of highest to lowest priority, these include, but are not limited to:

1. High Priorities – where records would be in danger of being permanently lost.
    - High Risk of Disposal – e.g.: Rubbish bins or bags, outside rubbish bins, waste disposal areas, shredding bags, etc…
    - High Risk of Theft – e.g.: Reception Areas, toilets, meeting rooms, consultation/examination rooms, other public areas
2. Most Likely Areas – where records would regularly be found

- Area records were last seen
- Area where records would often be found – e.g.: Record holder's workspace, regular records storage area (check for misfiling), colleague's work space, etc…

3. Potential Areas – where records could be found
    - Irregular storage areas – e.g.: areas where records could be stored but aren't normally.
    - Mobile storage – e.g.: Trolleys, carts, bags, boxes and crates
4. Any areas that the records were last in
    - Retrace record holder's "last steps"
    - Retrace record's last delivery or pick-up
5. Any areas that the records could be

This list is meant to be a very basic example. Real Coordinated Search Plans should try to include all the likely areas that the records could be in and as many of the unlikely areas as would be reasonable. Priorities should be set by the circumstances, but generally places where records could be placed so that they are permanently destroyed or removed (like the rubbish) should be searched immediately.

When searching the areas listed in a Coordinated Search Plan the date and time that the search was undertaken should be recorded.

5.13 Incidents and Reporting

The misplacement, loss, damage, theft or delay of Records may be a significant risk to the Care Trust. All staff should be aware of the following guidelines of reporting incidents in relation to Records Management issues.

5.13.1 What is an Incident

A primary method for the Care Trust to collect information about Records Management issues is through Incident Reports. While many situations such as the loss or delayed delivery of records may be common place throughout the Care Trust it may not be widely known or appreciated without the reporting of the situation. Incident reporting is therefore crucial to the Care Trust becoming aware of and dealing with issues of Records Management.

When reporting, staff should report confirmed, suspected or potential (Near miss) Incidents.

Not every issue is an incident however and reporting every single instance of missing records can become burdensome and overwhelm the Incident Reporting mechanism.

Issues that must be reported as an incident:

- theft, unauthorised accessing or viewing, unexplained loss or unauthorised receipt of Care Trust records or Care Trust information storage equipment;
- damage or unauthorised destruction of Care Trust Information or information storage equipment;
- significant loss of records or information storage equipment;
- significant delays to receiving records or existing information;
- threats, offers and bribes relating to gaining access to or for unauthorised use of Care Trust information;

- such poor quality of records that they are unusable for the purpose for which they were created.

Any Records Management issue that significantly affects or affected patient care, corporate functioning or the confidentiality of information must be reported.

Some issues should be considered in the context of how often they have been reported and how often it occurs. If the issue occurs constantly and has never been reported then there is a strong incentive to report. If the issue is infrequent but never reported then there is still strong incentive to report. If the issue is frequent and reported frequently, then it may be best to summarise a number of the issues into a single incident report rather than report on each incident. Issues to consider in this regards could be, but are not limited to:

- delays in receiving records;
- missing records;
- damaged records;
- overcrowded and/or unsafe and/or non-confidential storage space.

For Further information see the Care Trust's Incident Reporting Policy 2006.

5.13.2 Records Management Associated Incidents

Many Care Trust incidents have a number of contributory factors. Records Management may be included in a variety of incidents and not be recognised as such. When completing an Incident form all staff should consider the impact that Records Management had on the situation. For instance, medication errors could be based on not having the pharmaceutical records because the records were delayed, rather than an analysis of negative symptoms. Whenever appropriate ensure that if Records Management issues could have contributed to an incident that they are explicitly acknowledged on the Incident Reporting forms.

5.14 Records Rooms and Records Storage

Records and information are important assets for the Care Trust. Keeping them in protected environments is critical to their continued viability. There are considerable numbers of guidance documents and standards in existence outlining the requirements of safe records storage, particularly in respect to safe storage of electronic records. This policy does not intend to copy existing guidance, but instead provides what is required as a minimum within the Care Trust for the safe storage of records and information until such time as storage can meet appropriate external standards.

5.14.1 Access Control

All storage must have strict access control. This means that a limited and specifically empowered number of people have access and control over the records and information in a storage area. While all staff may have access to the records and information within, it does not mean that the storage system or space is under the control of everyone.

In order to meet this standard all storage spaces and systems must have:

- a published list of people who have access to the storage;
- a named lead for the storage.

A documented method of contacting the named leads or designated other person to gain access to the storage. This method should be submitted to the Records Manager.

5.14.2 Inventory Keeping

All storage sites and services must keep an inventory of the documents stored within. This inventory as a minimum should contain the types/categories, dates of closure for the documents being stored and the volume of documents in storage. All inventories must be kept up to date and submitted to the Records Manager at least annually.

Where practical, the ideal inventory should include for every item:

- a description of the documents;
- the date of the creation and where applicable, the date of closure;
- the person **and** service or directorate responsible for the documents;
- for electronic documents, the programs used to access the documents;
- any stakeholders that have access rights.

Any information that is relevant to the retention of the document

5.14.3 Minimum Security Features of Physical Storage

Physical storage must at minimum have the following characteristics:

- be secured from casual access by appropriate locks and barricades (ie: lockable doors and barred windows or lockable cabinets);
- have appropriate fire prevention and suppression mechanism/equipment;
- be free from damp and fluids, excessive heat, winds and animals/plants/fungus;
- provide adequate storage without damaging documents or electronic equipment;
- be safe and secure for staff to work in/with, including having at least annual risk assessments.

5.14.4 Minimum Security Features of Electronic Storage

Electronic Storage must at a minimum have the following characteristics:

- be secured from casual access by password protection, either that already inherent on a network or device, and where stored on a readable medium with no inherent protection, by password protection or similar encryption;
- have appropriate, structured, and identifying names, titles, security markings, warnings and/or confidentiality markings to prevent accidental deletion or access;
- have the author's name, responsible service and/or responsible directorate easily identifiable;
- have a back-up copy of the document stored separately.

5.14.5 Annual Audit of Records Storage

All Records Storage, physical or electronic, must be audited annually. This audit must report on the following:

- current volume of documents held against the total volume of storage available;
- a list of serious unauthorised accesses for that year;
- an update of the inventory.

The person(s) acting as the primary contact(s) and the responsible service and/or directorate for the storage.

5.15 Permanent Preservation of Records

The following section is guidance to assessing the value of a record for preservation. For further information, see the Care Trust's "Archiving and Destruction of Patients Records Policy February 2004".

5.15.1 Considerations to Retention Periods

The Care Trust is beheld to minimum retention periods for all of the records it creates. These minimum retention periods are primarily imposed by the Department of Health and other obligations may exists under professional standards, legal requirements, insurance standards, etc.

5.15.2 When should Records be Assessed for their Retention

Evaluation of Care Trust records for their historical value should occur at a number of points, not just at the end of the obligatory retention periods. "Milestones" in a records life should be used to make assessments of historical value and if done automatically at each "Milestone" the workload at the end of the obligatory retention period will be much lighter and much more effective. "Milestones" when the Care Trust will consider the historical value of its records will be:

- when the record is created;
- when the record is moved out of active service into temporary archives;
- when the record is moved into long term storage;
- when the record's obligatory retention period has expired.

All records must be assessed for permanent preservation or destruction no later than the 30th anniversary of the records closure.

5.15.3 Corporate Records we Automatically Keep for Historical Deposit

Many corporate records have great historical value. The following are already highly valued and have been requested by the London Metropolitan Archives:

- Board Meeting minutes and papers;
- major committee minutes and papers;
- major papers or documents (including strategies, unique performance assessments, project plans, annual reports, court decisions, etc…);
- Care Trust Internal Communications (newsletters, posters, publications, press releases, etc…);
- unique and significant documents (Royal correspondence, deeds, building plans, etc...);
- photographs;
- documents that have had the Care Trust seal placed on them.

The Care Trust has been requested to limit the frequency of deposits, with an appropriate deposit cycle every 20 years. The Care Trust will therefore ensure sufficient and safe storage of items until such time as the deposit.

5.15.4 Assessing Historical Value of Care Records

The historical significance of an individual care record is very small if one considers the vast amounts of similar records that exist. Although it is valuable to have a number of records about "average" service users with "common" care, the Care Trust will likely only find Archives willing to take in "exceptional" records. Characteristics that make records valuable are:

High Value:

- records detailing unique care methodology or technology;
- records of care that was the first usage of that methodology or technology of care in the UK or world;
- records of major celebrities or major public figures;
- records resulting from significant situations or events (e.g.: natural disasters, wars, major emergencies, etc…);

- records of rare diseases or disorders.

Medium Value:

- records of minor celebrities or minor public figures;
- records of care that was the first usage of that methodology or technology within the Care Trust;
- records of uncommon diseases or disorders.

Low Value:

- records of common care methodology or technology;
- records of regular citizens;
- records of common diseases or disorders.

When in doubt of the historical value of a record the Care Trust will contact The National Archive and/or the London Metropolitan Archive for an assessment of the records.

5.15.5 Where to Deposit

Care Trust records are already held by the London Metropolitan Archive, and as such any new records considered for permanent preservation will most likely have to be deposited with the London Metropolitan Archive.

Records that the London Metropolitan Archive declines but are still considered of value by the Care Trust will be taken to The National Archive for guidance on places of deposit.

5.16 Destruction of Records

Records not selected for permanent preservation will inevitable need to be destroyed. The following standards particularly apply to any type of records containing service user, personal or other sensitive information.

For further information, see the Care Trust's "Archiving and Destruction of Patients Records Policy, February 2004".

5.16.1 Selection for Destruction

All records, whether corporate or clinical will be assessed prior to the destruction to ensure that:

- the Care Trust is not obliged to keep the records under a minimum retention period or any other retention requirement or standard;
- the records have no significant historical value, or if they do have significant historical value, that every effort has been made to find a place of deposit without success.

Not all information needs to be destroyed via a formal destruction procedure. Information that is not sensitive, confidential or personal or subject to a minimum retention schedule may be destroyed outside of a formal destruction procedure. The following information **must** be destroyed via a formal procedure:

- information identifying a service users;
- information about Care Trust staff in relation to occupational health or human resources;
- information specifically named in any minimum retention schedule to which the Care Trust is beholden;

- any kind of information that is considered confidential. This can be considered by assessing the information against the exemptions to disclosure criteria of the Freedom of Information Act 2000. Should a record potential not be available under the Freedom of Information Act, then it is to be considered confidential.

5.16.2 Destruction Catalogue

Prior to destruction all records will be catalogued to ensure that the Care Trust can keep a record of all items that it has destroyed. This catalogue will be certified under secure procedures to ensure that no record is missed. No records can be removed from or added to the catalogued items list without it being noted on the catalogue. The items so catalogued must be signed off for destruction by the Care Trust's Records Manager or by a member of the Care Trust's Executive. Any Executive Director may authorise the destruction of records, however Directors may only authorise records that relate specifically to the services or information they are responsible for. The Director responsible for Records Management may authorise the destruction of any record or information.

5.16.3 Certificate of Destruction

All records destroyed will be noted by a certificate of destruction. Any certificate of destruction must be made in conjunction with the Destruction Catalogue such that together the Care Trust can clearly identify what records have been destroyed.

5.16.4 Security of Destruction

All records must be securely destroyed. This means that there are processes in place that enable the Care Trust to have no doubt that the records are completely destroyed. Such processes need to consider:

- security of storage areas;
- security of destruction areas;
- security of records being transferred for destruction.

If destruction is to be carried out by a third party the Care Trust must satisfy itself that, at all stages of destruction, including transport to the destruction site, safeguards are in place to ensure against accidental loss or disclosure.

The actual destruction process must also in itself be secure. Records must be completely destroyed, such that no readable information can be identified. Preferred methods of destruction will therefore include (singular or in any combination):

- incineration to fine ash;
- shredding to small size;
- pulping of paper to fine particles;
- puncture, smashing, magnetisation, heat damage and/or other irreparable damage to digitally held media, as appropriate to the medium.

5.16.5 Confirmation of Destruction

All destruction of records will be overseen and conducted by approved Care Trust staff or empowered third parties. Any of these aforementioned parties will certify that destruction has taken place by signing the destruction certificate.

5.16.6 Unauthorised Destruction or Records

Deliberate destruction of records may constitute a criminal offence, and will be, via this policy, a disciplinary offence within the Care Trust, regardless of the type of records or the medium which they were on. It will be at the discretion of any member of the Care Trust Executive to authorise these disciplinary processes. The Executive Director responsible for Records

Management has final decision on authorising disciplinary procedures. The Care Trust's Records Manager may request from the Executive Director for Records Management that disciplinary procedures be initiated.

6 TRAINING AND EDUCATION

- How will training or education needs be identified and met?
  - Review of requirements of policy vs. Staff Roles. Relevant staff assessed against policy requirements and training provided as required.
  - Assume all new staff need training.
  - Monitor LIs and SIs and records audits for breaches of policy, provide training as required.
  - It is expected that little skills training will be required, as all issues concern style and behaviour. Formal courses would be unnecessary.

7 DISSEMINATION AND IMPLEMENTATION

This document will be circulated to all managers who will be required to cascade the information to members of their teams and to confirm receipt of the procedure and destruction of previous procedures/policies which this supersedes. It will be available to all staff via the Care Trust intranet. Managers will ensure that all staff are briefed on its contents and on what it means for them.

- How will the policy/ guidelines be presented/launched/introduced in the clinical area?
  Policy to be sent to all Service Managers, all team/ward managers and considered at MDT/management groups. To be placed on intranet and communications to brief through Care Trust news.

- Will there be someone to contact for clarification or support in the implementation of the policy?
  Clarification and support for the policy will be made available through the Care Trust's Information Governance Manager/Records Manager and Clinical Governance Department. Both of these services can be contacted at the Care Trust's headquarters, St. Pancras Hospital. (020 7530 3500)

8 AUDIT

- Is there a clearly defined audit mechanism?
  The Clinical Governance Team supports a Trust wide Annual Case Notes Audit for all inpatient teams. A Trust wide Annual Case Notes Audit will be implemented in CMHTs during 2006/7. This audit considers the documentation and information within the case notes in accordance with this policy and CNST requirements.

  A baseline Records Audit was carried out across all teams within the Trust during 2005/6. This audit considers records management arrangements such as access and storage, again in accordance with this policy and CNST requirements. This will be re-audited bi-annually.

- How will the audit feedback be conveyed back to the staff implementing the policy?
  The results of the audit will be provided to the Clinical Governance Committee, the Records Management Committee and where applicable be incorporated into CNST re-evaluations of policy. Changes to the policy can be requested by any of these bodies to the Care Trust's Records Manager.

9 Review

Date/Trigger	Review Areas
Time Independent Reviews	

Timed Reviews	

10 REFERENCES

- Camden and Islington Mental Health and Social Care Trust – Code of Confidentiality For Sharing Client Information Within Community Mental Health Teams, August 2001.
- Camden and Islington Mental Health and Social Care Trust Access to Care Records Policy 2005.
- Data Protection Act 1998 and Freedom of Information Act 2000.
- Nursing and Midwifery Council Guidelines for Records and Record Keeping, January 2005.
- London Borough of Camden Social Services Good Practice in Record Keeping - Social Services Standards
- London Borough of Camden Social Services Access to User Records Policy & Practice Guidance
- London Borough of Camden Social Services File Retention Policy
- Camden and Islington Area Mental Health Committee Protocol for Multi-Agency Information Exchange, July 2000.
- Camden and Islington Mental Health and Social Care Trust - Care Programme Approach Operational Policy, April 2001
- Clinical Negligence Scheme for Trusts - Mental Health and Learning Disability Clinical Risk Management Standards, NHS Litigation Authority, June 2005.
- Government of England, Department of Constitutional Affairs – Data Protection Act 1998,
- Government of England, Department of Constitutional Affairs – Freedom of Information Act 2000
- CNST Standard for Mental Health, Standard 4, NHS Litigation Authority
- Camden and Islington Mental Health and Social Care Trust – Internet and Email Policy, 2005
- Camden and Islington Mental Health and Social Care Trust – Standing Orders Policy 2002

POLICY FEEDBACK FORM

POLICY TITLE	
POLICY REFERENCE	
DATE FOR REVIEW	
DATE FOR COMMENTS	

COMMENTS/SUGGESTIONS FOR POLICY REVIEW:
Areas to consider: local service developments, impact of policy on practice,