Camden and Islington NHS
Mental Health and Social Care Trust

ACCESS TO CARE RECORDS POLICY

FEBRUARY 2006

Camden ISLINGTON
supporting partnership in mental

POLICY TITLE	**ACCESS TO CARE RECORDS POLICY**
POLICY REFERENCE	COR6
POLICY CATEGORY	Corporate
RELEVANT TO	All Care Trust Staff
DATE PUBLISHED	February 2006
IMPLEMENTATION DATE	March 2006
DATE LAST REVIEWED	Not applicable
NEXT REVIEW DATE	February 2007
RESPONSIBLE PERSON	Tim d'Estrube, Information Governance Manager
CONTACT DETAILS	Email: tim.d'estrube@candi.nhs.uk | Telephone: 020 7530 3019
ACCOUNTABLE DIRECTOR	Claire Johnston, Director of Nursing Signature and date
APPROVED BY	Risk and Assurance Committee Date: 21/02/06
APPROVED BY	Records Management Committee Date: 04/10/05

DOCUMENT HISTORY

Date	Version	Amendments
01/02/06	1	

MEMBERSHIP OF THE POLICY DEVELOPMENT/ REVIEW TEAM	Timothy d'Estrubé, Information Governance Manager/Data Protection Officer
CONSULTATION	Information Manager
	Records Management Committee
	Caldicott Guardian

DO NOT AMEND THIS DOCUMENT

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

CONTENTS

1. INTRODUCTION/BACKGROUND

British Society is undergoing a transformation. Old cultures of providing information on a "Need to know" basis are recognised as obsolete and are being replaced by "Right to know" culture, a culture that accepts and supports the public's right to information about themselves and the organisations they support.

This cultural change is entirely relevant to Health Care and Social Care. No longer are care organisations and care workers able to exclusively retain service user information. Instead care organisations and care workers are stewards, maintaining service user information safely and effectively to the wishes of the service user, and according to the professional duties and the requirements of the law and society.

Primary to this role is the Data Protection Act 1998 and the Access to Health Records Act 1990. Collectively these pieces of legislation provide the framework in which all personal information of living and deceased people are kept, disclosed or withheld. These Acts are supplemented by British Common Law and NHS Directives. Although no less powerful than the Acts themselves, these are more fluid and practical, adapting the Acts to work in everyday situations. Finally there is the variety of professional guidance that different care working professions have for the creation, use and disclosure of personal information. Professional guidance important for care workers to know and follow, as it is the licensed framework in which to give care, provides legal protection and is useful as practical guidance.

Given the complexity of the situation it may be quite hard in any given circumstance to know what ones obligations are. This policy is therefore to assist the Care Trust in providing quality service to the public in balance with the requirements of legislation, law and NHS Directive.

This policy draws from a variety of sources, although it is primarily developed from the statutory requirements of:

- Data Protection Act 1998
- Access to Health Records Act 1990

As well as using guidance from:

- Information Commissioner

2. AIMS OF POLICY

This policy provides guidance in relation to the access of service user personal information in the form of Care Records. It outlines the obligations of the Data Protection Act 1998 and Access to Health Records Act 1990 as well as Care Trust duties to British Common Law and NHS Directives. Also provided will be the boundaries in which service user information is accessed by service users or third parties, and guidance on how access is granted. Public rights in relation to their personal information are explained and guidance is provided to fulfil these rights.

3. OBJECTIVES/SUMMARY OF POLICY

This policy is intended to:

- Ensure that the Care Trust protects and fulfils the Data Protection rights of service users' and the public.
- Summarise Care Trust duties in fulfilling Access to Information Requests under the Data Protection Act 1998 and Access to Health Records Act 1990.
- Provide a framework that the Care Trust can use to respond to requests for personal information about service users that is compliant with privacy and confidentiality laws.

- To provide teams and services frameworks to provide personal information formally with the support of a corporate service or informally under their own autonomy.
- Enforce practices that protect the Care Trust, its staff and its service users.
- Establish clear lines of management responsibility in regards to the access of personal information about service users.

4. POLICY SCOPE

This policy is intended only to provide guidance for the disclosure of information in response to a request made by an applicant. It is not intended to provide guidance for:

- Situations requiring unsolicited disclosure for reasons of professional conduct/codes, morality or ethics.
- Unsolicited disclosure of information under statutory or legal requirements (e.g.: Child Protection, registered communicable diseases, serious criminal offence, etc).
- Information arranged to be shared under Data Sharing Agreements, SLAs or other contracts, reporting for audits and commissioning, or similar prearranged transfers of information.

This policy does not attempt to incorporate profession-specific guidance or codes of conduct. It is expected that care workers should be familiar with their professional guidance. Although it is not expected that professional guidance will come into conflict with this policy, if it does any issues should be directed to the Care Trust's Data Protection Officer or the care worker's manager.

5. POLICY STATEMENTS

5.1 Forewords and Descriptions

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

5.1.1 Definition of Personal Data

Data

- Data or information created with the specific intent of capturing or recording opinions, facts, histories, views, etc… about a specific person.
- The definition of personal information is considered equivalent to the definition defined under the legal common law by the case: Michael John Durant v Financial Services Authority [2003] EWCA Civ 1746, Court of Appeal (Civil Division) decision of Lord Justices Auld, Mummery and Buxton dated 8th December 2003. (A full text of the judgment is available from the Court Service website at http://www.courtservice.gov.uk/)
- In this document, unless otherwise specified, "personal data" has the same definition as "personal data" and "sensitive personal data" of the Data Protection Act 1998.
- Synonymous in this document with "personal information" and unless otherwise specified, "data" or "information"

5.1.2 Definition of Data

Data

- Unless otherwise specified, same as "*Personal Data*" above.

5.1.3 Definition of Information

Information

- Unless otherwise specified, same as "*Personal Data*" above.

5.1.4 Definition of Records

Records

- Unless otherwise specified, a collection of information in any format or physical medium which is considered "*Personal Data*" (see above).

5.1.5 Definition of Public

Public

- For the purpose of this document the term "public" refers to any person or organisation that is not part of the Care Trust. This refers to service users, service user relatives, friends and representatives, other public authorities, government, legal or policing organisations, etc.

5.1.6 Definition of Applicant

Applicant

- For the purpose of this document the term "Applicant" refers to any person, institution or organisation that has applied for information from the Care Trust.

5.1.7 Definition of Processing

Processing

- For the purpose of this document the term "Processing" refers to any use, storage, creation, evaluation, summarisation, disclosure, withholding separation, amalgamation or destruction of information about service users.

5.2 How to use this Guidance

This guidance is primarily for use with health and social care information held by the Care Trust. It does however have partial relevance to other types of personal information. The following sections of this document apply to any type of personal information request.

Sections:

- 5.4 – Obligations of the Data Protection Act
- 5.6 – General Procedure for formal Requests for Personal Information
- 5.8 – Creating a Formal Written Request
- 5.9 – Receiving a Request

This document is divided into sections that overlap each other. Ideally the reader would read through the entirety of the document once to get an overall understanding, thereafter only needing to use the table of contents and descriptive column on the left hand side to locate pertinent information.

5.3 Responsibilities within the Care Trust

This section outlines the responsibilities of the Care Trust in terms of the Data Protection Act 1998 and the Access to Health Records Act 1990. It defines the responsibilities at various levels and positions throughout the Care Trust.

5.3.1 Data Protection Act responsibilities at Board Level

For the purpose of the Data Protection Act 1998 the Care Trust Board has the same legal responsibility for the actions of the Care Trust that Executive Directors have. This responsibility exists only in relation to the Board members' management area, and not as a Care Trust whole.

5.3.2 *Responsibility for the policy at Board Level*

The Board is also responsible for endorsing this policy and ensuring that the policy is implemented throughout the Care Trust. This includes providing adequate resources for the processes that support this policy and providing appropriate empowerment to the posts and processes involved.

5.3.3 *Chief Executive Responsibility*

The Chief Executive has overall responsibility for the Care Trust regarding the provision of information. By statutory requirement, clear lines of responsibility must be drawn from every staff member to the Care Trust Executive for the provision of information. Note that in certain situations members of the Care Trust Executive may carry the penalties for improper disclosure or retention of information personally.

The Chief Executive has the additional responsibility of being the last avenue of appeal within the Care Trust for complaints relating to Data Protection.

5.3.4 *Director Responsibility*

Directors have the responsibility for:

- Ensuring that their directorates and departments are fully aware of their responsibilities and that the directive's processes and policies support this policy.
- Ensuring that their directorates and departments provide Data Protection Services appropriately and in a timely manner and will be responsible for the decisions and responses their directives and departments make.
- Ensuring that the directorates and departments are adequately resourced so that they do not present a barrier to accessing information.
- Investigating those complaints and disputes under this policy which involve their services or departments.

5.3.5 *Caldicott Guardian Responsibility*

The Caldicott Guardian has the responsibility for:

- Ensuring that adequate policy and guidance is provided and followed for the transfer of personal information to the public or other organisations and that any policies and guidance work in concert with this one.
- Enabling, in conjunction with the Lead for Data Protection, resources to be available to staff who provide personal information to support their queries and best practice.
- Development and maintenance of this policy in conjunction with other areas of relevant expertise (e.g. Data Protection Officer).
- Fulfilling the responsibilities given in this policy (esp. Further Guidance).

5.3.6 *Senior Management Responsibility*

Senior Managers have responsibility for:

- Ensuring that the services and staff they are responsible for are educated in this policy and its supporting policies, and that these policies are adequately enforced locally.
- Ensuring that local processes, policies and staffing do not present a barrier to the accessing of information.
- Ensuring that they are adequately aware of the policies and procedures for accessing information to enable them to support staff in decisions regarding access to information

5.3.7 Data Protection Officer

The Data Protection Officer has responsibility for:

- Development and maintenance of this policy in conjunction with other areas of relevant expertise (e.g. Caldicott Guardian).
- Being a primary contact for this policy.
- Being a resource for the development of local procedure and policy for accessing information.
- Fulfilling the responsibilities set out in this policy (esp. Further Guidance).

5.3.8 Local Manager and General Staff responsibility

Local managers and general staff have responsibility for:

- Ensuring that they and staff under their management are adequately trained in and follow procedures and policy.
- Ensuring that local processes, policies and staffing do not present a barrier to the accessing of information

5.3.9 All Employees of the Care Trust

All employees of the Care Trust have responsibilities for:

- Maintaining the spirit of the exercise; To provide an open, honest and accountable Care Trust that services the public's Right to Know in balance with the respect for individuals' confidentiality and privacy of their personal information.
- Feeding back issues through their line management whenever this policy is in conflict with professional values, legal or statutory obligations and/or is generally impractical.
- Ensuring 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 identified appropriate resources.
- If receiving a request for personal information and have no authority to handle it themselves, contact the Data Protection Officer or the Information Request Office immediately (written requests must always be sent to the Data Protection Officer).

Information Request Office
Camden and Islington Mental Health and Social Care Trust
Room 120, 1st Floor, East Wing,
St Pancras Hospital
4 St Pancras Way
London NW1 0PE

Phone: 020 7530 3019
Fax: 020 7530 3021
Email: Information.Request@candi.nhs.uk

5.4 Obligations of the Data Protection Act 1998

This section outlines the requirements of the Data Protection Act in relation to the public's rights of accessing and controlling personal information as well as the Care Trust's rights when receiving a request.

5.4.1 Background

The Data Protection Act 1998 grants the public unprecedented access to personal information. With only a few exceptions the public can request either copies or viewings of any opinion, biographical record or assessment made specifically to record information about them held by any UK organisation. They further have the right to request changes to be made to information that is deemed erroneous, unfair, incomplete, irrelevant or outdated.
The Act also grants specific rights relating to electronically held information and its processing such that the public can request human intervention into automated decision making and where appropriate removal or deny the creation of electronically recorded information.

The Data Protection Act is intended to apply to the data of the living; however the Department of Health has given the directive that the living and deceased people have the same rights to expect privacy and confidentiality. What remains of the Access to Health Records Act 1990, after the majority of it being superseded by the Data Protection Act 1998, applies only to the data of the deceased.

5.4.2 Summarised Access Rights of the Public

The public has the right to request, and where appropriate receive, the following in relation to any appropriate information about themselves held by the Care Trust:

a. To know if personal data relating to themselves is being held or processed by, or on behalf of, the Care Trust.

b. Be given a description of the information held, including:
   i. the purpose for which the information is held;
   ii. the people or type of person who may receive the information.

c. To be provided with:
   i. the information itself;
   ii. any information relating to the source or acquisition of the information.

d. To know the logic by which any evaluation is made of the information that relates to matters directly concerning the individual.

e. Receive a permanent copy of the information unless otherwise impossible, unrealistic or a copy is not requested.

f. Receive sufficient explanation of any information provided as required.

g. Receive the information as it was at the time the request was made, with the exception of any changes that would have been made subsequently regardless of a request being made or not.

5.4.3 Summarised Control Rights of the Public

The public has the right to request, and where appropriate, receive control over the use and dissemination of any appropriate information about themselves held by the Care Trust:

a. Change, delete* or add information to that held by the Care Trust on the grounds it is erroneous, unfair, incomplete, irrelevant or outdated.

b. Provide or restrict access to the information in relation to any third party or between distinct units of the Care Trust including the sealing of information to be accessible only under specific circumstances.

c. Require human intervention and evaluation in decisions that would otherwise have been done by an automated process.

*Usually only under extreme circumstances of significant risk to the subject of the information can information be removed from a health record.

5.4.4 Summarised Rights of the Care Trust

The Care Trust has the following rights when granting access to information under the Data Protection Act 1998:

a. Refuse a request if it has not been provided in writing.

b. Refuse a request regarding unstructured information* that would exceed the maximum cost allowed for a request for information as legislated under the amendments to the Data Protection Act 1998 by the Freedom of Information Act 2000 (currently £450.00).

c. Prescribe a fee, not exceeding the maximum cost allowed under the Data Protection Act 1998 (currently £50.00).

d. Refuse a request if the identity of the requestor is not satisfactorily provided.

e. Refuse a request if the request does not provide sufficient information to identify the requested information.

f. In most situations, refuse to provide information about a third party if the third party has not provided consent to disclose their information.

g. Refuse a request if previous requests have been identical or substantially similar and the information has not subsequently changed or there has been insufficient time since the last request.

* Unstructured information refers to information held, sorted or filed in ways that do not readily identify information about a specific person.

5.4.5 Summarised Rights for Duty of Care

The Care Trust has the obligation to consider the best interest of the service user, public and any third party when providing information for disclosure. When appropriate the Care Trust must withhold information that it holds where it believes that the information would cause significant harm to the mental or physical health of any individual.

5.4.6 Summarised Rights of the Care Trust to provide treatment in conjunction with Records Management

The Care Trust has the professional and ethical obligation to provide safe treatment and care to the public. Part of the necessary process in providing care is the creation and use of information, in this case the health record. Where the creation or use of the health record has been specifically denied or obstructed by the expressed wishes of the service user, to such an extent that the Care Trust cannot provide safe and/or ethical treatment, it has the ability to deny treatment.

Treatment can only be denied where the lack of information, or the restrictions of communicating known information places the service user at risk, the Care Trust at risk, or the any other person at risk.

5.5 Obligations of Access to Health Records Act 1990

This section outlines the requirements of the Data Protection Act in relation to the public's rights to access and control personal information of deceased people as well as the Care Trust's rights when receiving a request for the information about deceased individuals.

5.5.1 Background

The Access to Health Records Act 1990 originally governed all aspects of accessing the Care Trust Care Records. With the implementation of the Data Protection Act in 1998 most of the Access to Health Records Act 1990 was overwritten. The surviving pieces of the Act now only apply to accessing the records of the deceased.

The Access to Health Records Act is basically the same as the Data Protection Act 1998 in terms of the publics' requirements for making a request. The two Acts are significantly different in that the 1990 Act only applies to the information about deceased individuals, there

is also no obligation on the part of the Care Trust to provide justification for the creation or use of records and there is no ability for a third party to restrict or control the processing of the information. Additionally when the public applies for information about deceased people, they must supply the Care Trust with justification of their need to access the record.

5.5.2 Summarised Access Rights of the Public

In combination with a legitimate need for information the public has the right to apply for, and where appropriate receive, the following in relation to any appropriate information about a deceased person held by the Care Trust:

a. To know if the requested information is being held or processed by, or on behalf of, the Care Trust.

b. To be provided with the information itself.

c. Receive a permanent copy of the records unless otherwise impossible, unrealistic or a copy is not requested.

d. Receive sufficient explanation of any information provided as required.

5.5.3 Summarised Control Rights of the Public

The living public has no ability to control access to the information of a deceased person. However the Care Trust must consider prior wishes of a deceased person when access to their information has been requested. Access control remains entirely with the Care Trust, which is obliged to follow the tenets of the Access to Health Records Act 1990.

5.5.4 Summarised Rights of the Care Trust

The Care Trust's rights in relation to a request for personal information about a deceased person remain the same as those under the Data Protection Act 1998. This is with the exception of the additional conditions of:

a. The ability to refuse a request if the request does not provide sufficient explanation of the requestor's legitimate need to access the deceased information

b. The ability to refuse a request if the Care Trust does not believe the need to access the deceased persons records as explained within the request outweighs the right to privacy of the deceased person.

5.5.5 Summarised Rights for Duty of Care

The Care Trust has the same duty of care to the living public and third parties in preventing significant harm to any individual when releasing information. There is no obligation for duty of care to deceased people or deceased persons' previous interests.

5.6 General Procedure for a formal Requests for Personal Information

This section provides an outline of the general procedure in the Care Trust when a member of the public makes a request for personal information.

5.6.1 Receiving a Request

The Care Trust must by law be able to process a request for personal information regardless of which of its employees receives it. To enable this to happen the Care Trust has centralised the request process by having all written requests sent to the Data Protection Officer at the Information Request Office.

Once a request has been received it should have the following either written directly on the request or have an accompanying document stapled to it:

- the date it was received;
- the person who received it;
- any additional information necessary.

There is a statutory expectation that the Care Trust responds to requests within 40 calendar days so on receipt of the request, it should be immediately sent to the Information Request Office. The address is:

Information Request Office
Camden and Islington Mental Health and Social Care Trust
Room 111, 1st Floor, East Wing,
St Pancras Hospital
4 St Pancras Way
London NW1 0PE

Phone: 020 7530 3019
Fax: 020 7530 3021
Email: Information.Request@candi.nhs.uk

It is only necessary to fax or scan and email a document if it will not arrive within two working days, or if the request was not immediately sent on being received.

5.6.2 Processing a request

Once a request has been received at the Information Request Office, the Data Protection Officer will do the following:

- Provide a brief acknowledgement of the request to the applicant.
- Assess the request to see if it can be granted.
- If the request is not possible to process due to problems with the request or a lack of information, contact the applicant for more information.
- Where an application is inappropriate to process contact the applicant with an explanation.
- Where appropriate, pass the request to Caldicott Guardian.

In short the Data Protection Officer will act as the liaison between the applicant and the Care Trust to ensure that the clinical or service team do not need to be involved with the details of the Data Protection Act or Access to Health Records Act. The Data Protection Officer may liaise with teams and services to assess the request, and where appropriate request that the service or clinical team act as the liaison or enter into discussion with the applicant themselves.

In instances of providing information to other organisations or institutions it is the responsibility of the Caldicott Guardian to authorise the transfer of requested information to the other organisation. The Data Protection Officer will assess where the responsibility for a request lies between the Data Protection Officer and the Caldicott Guardian, and where appropriate pass the request to the Caldicott Guardian.

Teams and services will be given instruction by the Data Protection Officer or the Caldicott Guardian as to how the information will be prepared for disclosure.

5.6.3 Providing Access

Information holders will be responsible for providing access to the records under the direction of the Data Protection Officer. Once a request has been approved the Data Protection Officer

will contact the information holders and provide instructions as to how the request is to be met. All clinical teams will be expected to arrange third party permissions, viewings, copying of information and where appropriate transportation/delivery of information. The only exception to this is for viewings in the context of limited staffing arrangements of outpatient clinics. In this instance if the outpatient care worker is unable to provide time for a viewing alternative arrangements can be made. The Data Protection Officer has sole discretion over whether alternative arrangements will be provided.

5.7 Informal Requests

Many applications for personal information will not be in the form of formally written requests. Where possible, clinical teams should attempt to satisfy small and easily handled requests to enable the public to have quick and easy access to their information. The following gives some guidance and limited autonomy to do so.

5.7.1 Autonomously and informally handling of requests by teams and services

Where a request is small and easily provided teams and services are enabled to provide personal information. All of the following conditions must be met however:

- The Information Holder is 100% certain of the identity of the person.
- The applicant is applying only for information about themselves (OR the applicant is certified to be the legal representative of the subject of the information AND consent has been explicitly given in writing by the subject of the information).
- The information to be supplied does not contain any information provided by or about a third party and does not contain any information that would be harmful to the mental or physical health or significant interests of any person or the Care Trust.
- If copies are to be made, the number of copies is not significant enough that the information holder would apply a charge for the materials (recommended to be volumes of less than 50 pages).
- Any copies to be given are to be provided in person to the applicant.
- There are no issues of capacity for the applicant to provide consent for a third party to see the information, regardless if a third party being named or present.
- If a viewing is required, the time and supervision required for a formal viewing can be appropriately provided (See Section Releasing Information as Viewings).
- The person making the decision to provide the information has the seniority to do so.
- Either the service or team manager, or the Data Protection Officer has been notified.

5.7.2 Situations of Requests which must be handled formally

Teams and services must **not** handle informal request for personal information if they involve any of the following:

- The applicant requests information about someone else (except for legal representatives under the specific circumstances outlined above).
- The requested information is about a deceased person.
- The applicant is requesting information for a third party to see on their behalf and there are issues with the capacity of the service user to provide such consent.
- The applicant is unknown to the team or service.
- The request requires a volume of copying of information sufficient to warrant charging the applicant.

- The information requested contains third party information, was supplied by a third party or contains information potentially or actually harmful to any other person.
- For any other reason the team or service does not want to handle the request informally.

In these instances the team or service must provide the instructions as to how an applicant can make a formal written request for information.

5.7.3 Team/Service Choice to provide information for an informal request

Teams and services are not required to provide information for an informal request and have sole discretion for doing so. However if a refusal is made the team and service must provide the instructions as to how an applicant can make a formal written request for information.

5.7.4 Care Trust clinical practice encouragement

The Care Trust encourages all care providers to share the records that they make on a service user in an informal way. Although this may not always be possible due to the sensitivity of certain information or situations, the Care Trust encourages the sharing of clinical information with the subject of the records as part of the care/treatment process. Suggested examples include:

- Outpatient user settings: If notes are made during a session, allow the client to view the notes prior to the end of the session. If notes are made after the end of the session, allow the client to view the notes of the previous session or making the notes available in future sessions.
- Inpatient user settings: Allow the client to view information collected throughout the stay at appropriate quiet times in the day.
- Beginning of Care: If appropriate, provide the information that was provided to the service at the beginning of a care episode. This can be particularly important to catch errors or inaccuracies that may affect the care to be offered in the upcoming episode.
- End of Care: At the end of the care episode, allow the client the opportunity to view the notes prior to leaving care. Use the last sessions to review the notes as part of the closure of care.

5.7.5 Formal non-written requests

In some cases applicants will not be able to provide a written request. If a written request cannot be provided but the applicant is formally requesting a viewing of their information the Care Trust has an obligation to provide reasonable assistance in creating a suitable request. Teams and services should be prepared to assist the applicant but if assistance is not practical the applicant should be given the contact details of the Information Request Office and the Data Protection Officer.

5.8 Creating a Formal Written Request

This section outlines what a formal written request should contain.

5.8.1 Checklist for a Request

A formal written request must at minimum contain the following information in order for it to be a valid and useful request:

- Provide the full name and contact address of the Applicant, and if different from the Applicant's, the full name and address to which the information is to be sent.
- Be legible and usable for locating the information requested.
- Be informative enough on its own that it can be used for subsequent reference.
- If possible, the signature of the applicant.

In the event where the applicant is a third party they must also provide either:

- Written consent from the subject of the information; or
- The authority under which they have the right to request the information

In the event where the applicant is requesting information about a deceased person they must also provide:

- Information justifying the reason they require access to the information.

5.8.2 Acceptable formats of a written request

A written request can be received in the form of a letter, fax or email.

5.8.3 Care Trust Forms

The Care Trust has produced a form for public use when requesting personal health and social care information. This form can be found in the Care Trust's Document Store. The Document is named: Application for Access to Care Records Form and can be found in the "Corporate Information" section of the document store.

There are currently no other forms available for the request of information other than care records.

5.8.4 Considerations when assisting in creation of a formal request

When assisting in the creation of a request it is helpful to consider the following:

- In the interest of time and costs to the Care Trust and the applicant, is there specific information of interest that could be requested rather than all information?
- Viewings are essentially free to the applicant and can be a good way of reducing the copying costs by selecting what information is of interest for copying.
- Would the information be inaccessible because it was provided in confidence by a third party, or the information is about a third party?
- Is there sufficient information to identify the authority under which the information is being requested?

5.9 Receiving a Request

This section describes the responsibilities of staff when they receive a request for personal information.

5.9.1 Expectations on Staff receiving an Information Application

A request for personal information can be received by any staff member of the Care Trust. Upon receiving a request a member of staff will as soon as is practical:

- If the request is written, record the date received, the person receiving it and any other relevant information, then immediately forward the request to the Information Request Office:

  Information Request Office
  Camden and Islington Mental Health and Social Care Trust
  Room 111, 1st Floor, East Wing,
  St Pancras Hospital
  4 St Pancras Way
  London, NW1 0PE

  Phone: 020 7530 3019
  Fax: 020 7530 3021

Email: Information.Request@candi.nhs.uk

- If the request is not written, inform the applicant that they need to provide a written request and:
  - Provide information on where to find guidance, or provide the guidance and advice themselves on what an acceptable request would be.
  - Provide the contact information for the Information Request Office.
  - Provide other reasonable assistance to ensure that either the Application or the Applicant's contact information reaches to the Information Request Office.

A staff member receives a written request the day it arrives in their electronic or physical Inbox or are otherwise contacted.

Members of staff must **not**:

- Provide the information if they are not authorised to do so, and if they are authorised to do so, will not provide the information without contacting the Information Request Office or their manager.
- Inquire into the reasons, motivations or intentions of the applicant for asking for the information unless they are authorised to provide information and need to ask only for the reason to clarify what information is requested.
- Make the judgement themselves, without instruction from the Data Protection Officer or their manager, and refuse the request on the grounds that the request is vexatious, repeat or for inappropriate information.

5.9.2 Expectations on Staff seeking Information

A member of staff seeking their own personal information for reasons not related to their work will not take the information even if they hold it. Members of staff wanting their own personal information are required to submit a formal written request to the Information Request Office as per normal.

5.9.3 Requests other than from a member of the public

Requests for personal information can be received from a variety of sources. These include police, local authorities, government, media, companies, courts, lawyers, etc. Unless specifically instructed otherwise, these requests must be sent to the Data Protection Officer or Caldicott Guardian. The Data Protection Officer can be reached at the Information Request Office (see contact details above). The Care Trust's Caldicott Guardian is:

Medical Director/Caldicott Guardian
Camden and Islington Mental Health and Social Care Trust
2nd Floor, East Wing,
St Pancras Hospital
4 St Pancras Way
London NW1 0PE

Phone: 020 7530 3076
Fax: 020 7530 3083

5.10 Data Sharing Agreements

In some instances these requests would be handled under predefined protocols. These Protocols, known as Data Sharing Agreements, must be fully understood by staff prior to the release of information.

5.10.1 Use of Data Sharing Agreements and this policy

Data Sharing Agreements' protocols for sharing specific information override some or all of the guidance and requirements of this policy. Where the information requested is different from that which the agreement can provide, or has been requested by or is to be sent to a party that are not named within the agreement, the request automatically falls outside of the Data Sharing Agreement and must be treated as a basic request and dealt with in accordance with this policy. Any questions about whether a request falls under a Data Sharing Agreement should be directed to the Caldicott Guardian.

5.11 Preparing for Release of Information

In most cases information needs to be vetted prior to release outside the Care Trust. This vetting prevents disclosure of information confidential contributed to a care record as well as protecting the health and safety of service users and members of the public.

5.11.1 Reasons to vet information

It is critically important to vet information prior to its release. It is done to protect members of the public from potentially serious damage to reputation or physical and/or mental health and to protect the Care Trust from loss of public confidence and legal challenges.

5.11.2 Legal Implications of releasing personal information

An individual who is seriously harmed by the inappropriate release of personal information can take the releasing organisation to court. Under the law, not only is the organisation that was responsible for the release of the information liable, but the individuals within that organisation who authorised the release of the information can be personally liable as well.

Where the release of information was done properly with all appropriate considerations, but resulted in a prosecution due to serious harm, the Care Trust will provide sufficient support to staff responsible for the information's release. If information was inappropriately released or without proper procedure or care, the Care Trust will not necessarily provide support to the staff responsible for the release.

5.11.3 Responsible positions for Vetting Care Information

When reviewing health and social care information for release the most relevant care worker involved in an individual's care must review the notes, summaries and reports and any other information eligible for release. In some cases the original care worker may no longer be available to vet the information, at which point the responsibility for vetting the information must be passed up the management chain. Although a there are a number of different situations in which care records may be considered for release, the following hierarchy should be considered for who would be the most relevant person to vet the information when passing the responsibility upwards.

Suggested Staff Responsible for Vetting Information (Listed in descending order)				
Level of Involvement with Service User	**Community Services Scenario**	**Inpatient Services Scenario**	**Outpatient Services Scenario**	**Other Services Scenario**
Directly Involved	Care Worker	Consultant, SPr or SHO	Care Worker or Consultant	Care Worker or Consultant
Service Involved	Other Team Members (must be Care Workers)	Consultant (RMO)	Other Team Members (must be Care Workers)	Other Team Members (must be Care Workers)
	Team Manager	Ward Manager	Team Manager	Team Manager
Managers Involved	Service Manager	Service Manager	Service Manager	Service Manager

	Service Director	Service Director	Service Director	Service Director

Vetting individuals they need not have written the notes or even be familiar with the individual the information is about. It is strongly recommended however that if the vetting individual does not know the individual the information is about that they should consult with the care workers directly involved with the care of the individual. If the original care workers are not available, similarly qualified people who would be familiar with the services or profession involved in providing the care recorded by the information is advised.

5.11.4 Assistance for vetting

The individuals responsible for vetting information for release may seek assistance from any qualified member of the Care Trust. This may include empowering other individuals within the Care Trust to do the vetting on their behalf. **It is important to note that when empowering other individuals to vet information, the legal responsibility for releasing the information remains with the empowering individual.**
Qualified members of the Care Trust refer to any individual or organization employed, contracted or otherwise officially and legally working for the Care Trust who has qualifications relevant to the information being vetted (i.e: Nursing Records could be vetted by a Care Trust Nurse). Assistance must not be sought from any individuals or organizations who are not employed, contracted or otherwise officially and legally working for the Care Trust and to knowingly do so will be considered a breach in the Care Trust's Code of Confidentiality.

Although seeking assistance is encouraged, it is best to limit the number of assisting individuals to the absolute minimum to preserve the confidentiality of the care record. Where a service user has provided specific instructions that their care records are not to be seen by a particular individual or group who the vetting person believes must participate in the vetting procedure, the Data Protection Officer or Caldicott Guardian should be contacted for advice.

5.11.5 What to look for when vetting information

Under the Data Protection Act 1998 and the Access to Health Records Act 1990 the only health and social care information that is to be considered for withholding from release is:

- Third Party Confidential Information.
- Information that would cause significant harm to the mental or physical health of any individual.

No other information can be considered for withholding.

Information of these types must be treated separately and in many cases removed from health and social care information prior to release outside the Care Trust.

It is worthwhile noting that penalties for disclosing information inappropriately are generally much worse than inappropriate withholding; however it is usually far easier to be penalised for withholding than disclosing.

5.11.6 Definition of third party Information

Third parties are any organisation or individual that is not the subject of the information or are not part of/an employee of the Care Trust. The Care Trust is considered one organisation regardless of the numbers of specific teams, units or individuals that produced/provided the information being vetted. Therefore no information produced within the Care Trust can be considered as third party information for the purpose of vetting care records. Third party information is information that is any or all of the following:

- Information provided in confidence and would constitute a legal breach of confidence if disclosed.
- Information that is about a third party.

- Information that reveals the identity of the third party even if the third party is not specifically named (e.g.: Childhood stories provided by a relative may identify the relative because they would be the only ones to know those stories).

Note that records made by a care worker providing a client any sort of care, regardless if:

- the care worker works in private or public healthcare;
- the care worker is a member of Care Trust staff or not;
- the care was provided for the Care Trust or not is information that is not to be considered as third party confidential information and must be considered for release.

Where third party information exists, the third party's wishes in whether to release the information must be explored. This will often necessitate contacting the third party to ask permission.

5.11.7 What to do when third party confidential information is found

Third party confidential information is not necessarily withheld from release. It is the duty of the vetting care worker to make a reasonable effort to contact the third parties to request permission for the information to be provided to the applicant. Where the third party approves of the release of information, the information is not considered to be confidential for this request. In the event that the third party denies permission, the vetting care worker must edit the information, or provide a summary of it, that would remove the third party reference such that the third party could not be identified but the rest of the information was available. If the third party cannot be contacted, the vetting care worker needs to consider the following in determining if the information is suitable for release or not:

- Previous refusals for permission to disclose or standing consent for disclosure.
- The duty of confidence owned to the third party.
- Perspectives on disclosure from a suitable representative of the third party.
- If it is reasonable in the circumstances to provide the information without the consent of the third party

Vetting care workers are cautioned that if they cannot contact the third party to receive permission to disclose, they should withhold the third party information.

Information deemed to be third party confidential must be withheld from disclosure.

5.11.8 Definition of Harmful Information

It is a professional care decision whether information will cause harm to any person. A judgement must be made by a qualified care worker in good standing with their professional regulators and employed by the Care Trust. By law the professional judgment of potential or actual harm a piece of information carries requires the same personal responsibility (i.e.: Duty of Care) as the act of providing care. In instances where the individual responsible for vetting the information is not a care worker the responsibility for disclosing harmful information remains even if they have asked for vetting assistance and relied on advice from a care worker.

A care worker is therefore personally responsible for a decision of harmfulness (or harmlessness) and can be personally held responsible for their judgement. It is good practice to consult with other care workers who have provided information to ensure that from the collective insight into the subject that all areas of potential harm are covered. "Harm" can only be generally defined given the vast range of personal circumstances that an individual with care records could have. That said there are two core qualities that must be considered to define information as "harmful":

- "Harm" must be potential in the future, and not already have happened or is already occurring.
- Common law suggests "Harm" should only be considered when it would be very significant, such that a person would threaten their life or the life of another. Severe self-neglect, suicide, homicide or any other condition that would put someone into hospital would comfortably qualify as "Harm". Abuse or neglect of children or other adults may also be considered "Harm" although this would need to be considered carefully. Exposing family secrets (i.e.: "That is not your real father") would be considered serious harm. Serious offenses that would result in imprisonment may also be considered harm.

Not all information will be harmful to all people, however the Duty of Care is always to the person accessing the records. For instance, a Care Trust service user provides consent to their partner to access their records. Within it is information potentially quite harmful to the partner, but not the service user. The vetting care worker would therefore vet the notes to protect the partner from harm, and not the service user, unless there was information that would harm the service user if the partner knew it. Vetting information in these particular situations can be confusing and as such the Data Protection Officer and the Caldicott Guardian are available for questions.

5.11.9 What to do when potentially harmful information is found

Where information is considered potentially harmful to a person other than the applicant it must be withheld.

Where information is potentially harmful to the applicant, the potential for harm must be weighted against the applicant's right to informed consent for their treatment and their Data Protection rights.

Where individuals receiving care request to have access to their records it is helpful to consider the following:

- Do the individuals have the capacity to understand the implications of the harm the information may cause them?
- Does the individual's need for protection outweigh their right to informed consent for treatment?
- Does the individual's need for protection outweigh their rights to receiving their personal information under the Data Protection Act 1998?
- Will the reaction to the information genuinely cause them harm or will it only complicate the care being provided/lead to withdrawal from the service?

Information deemed to be harmful must be withheld from disclosure.

5.11.10 What to do when information is removed

If during the vetting process information is discovered to be unsuitable for reasons of third party confidentiality or potential harm then it must be removed from the information prior to its release to the applicant.

Documents in themselves are not to be considered for withholding. It is the information that a document contains that is to be considered. Therefore if there are ways of altering information such that it can be disclosed without risking third parties or serious harm, and without changing what the information is about, then the creation or alteration of a second document must be considered. The consideration for vetting therefore is how to change and or rebuild a document so that it complies with the above requirements and releases as much appropriate information as possible.

In this instance where information is to be withheld from disclosure the individual responsible for vetting the information is responsible for:

- Withholding only as much information as necessary to preserve the confidentiality of third parties and prevent potential harm from occurring.
- Provide a general description of the information to be withheld and the justifications for doing so. Note that the descriptions and justifications must not expose the information that is being withheld. If it is impossible not to expose the information by releasing a description then the information may be entirely withheld. This general description and justifications must be kept with the care record it refers to and must be produced for the applicant whose request is being refused/partially refused.
- **Ensure that the justifications for withholding information are included within the care records of the individual for future reference.**

There are significant risks to service users, care workers, and the Care Trust if justifications for withholding information are not recorded. Failure to record the justifications for withholding information within the care record will be seen a breach in this policy and in the Duty of Care to the service user.

5.11.11 Explanatory information requirement

It is required by the Data Protection Act and Access to Health Record Act that in the event of providing information it must be understandable by the recipient. Where it is the belief of the provider, or expressed by the recipient, that the recipient does not understand the information being provided, the Care Trust must provide sufficient guidance and information to assist the understanding of the recipient. This can be done either by providing a glossary of terminologies and explanations of procedures/diagnoses or allowing the recipient to otherwise ask questions to the Care Trust. In either case it is the team or service that is responsible for the information that must provide this extra information.

5.11.12 Justification/Usage information requirement

It is a requirement of the Data Protection Act that if the recipient of information requests to know why specific information was recorded and used that the Care Trust provide justification for its recording and usage. The answers to the recipient's questions should be as detailed and specific as the question, hence providing the response of "recorded and used for the purpose of providing care" to any questions may not be appropriately detailed enough. In the event of such questions being asked it is the team or service that is responsible for the information that must provide this extra information.

5.12 Consent, Sealed Information, Advanced Directives, Guardians

Information held by the Care Trust may have specific instructions/restrictions attached in relation to its release or usage. These instructions will almost always be given by the individual the information is about, and in most cases must be respected. Service users may also have appointed guardians or representatives that are empowered to make decisions about their information on their behalf. These guardians must be respected in the same way as a service user is.

This section provides guidance when there are given consent and standing instructions from the subject of the information or their guardians to consider when vetting information for release.

5.12.1 Sealed information

In some instances service users request information to be sealed, and only opened for specific reasons or in particular circumstances. In these instances, unless the instruction is otherwise, this information will remain sealed and not disclosed for regular Data Protection requests by third parties. If appropriate the individual responsible for the vetting can regard the information as though it were third party information and seek permission for its disclosure

from the service user. This is not the case for requests the Care Trust has statutory obligation to provide for, such as police requests, child protection inquiries, court orders, etc.

When vetting information, the individual responsible for the vetting must decide whether to open the sealed information so that they may assess the contents for disclosure. Under normal Data Protection requests, not involving a statutory gateway (see section: Statutory Gateways for third party access to information) it would be inappropriate to break the seal. If the information is opened and vetted, the individual responsible for the vetting must:

- Limit contact with the information to as few people as possible.
- Record when and why the seal was broken.
- Record if the information was released and why and to whom it was released.

Where there is sealed information and it is not provide in a disclosure, a simple description such as "Patient sealed information of unknown content" and a justification of "Withheld on service user's instructions" will suffice for the documentation of withheld information to the application (see section: What to do when information is removed).

5.12.2 Consent for third parties to access information

Care Trust service users may request that third parties have access to their records. In most cases this may be appropriate, however the Care Trust must assess capacity if the service user is currently receiving care from the Care Trust, or the Care Trust is aware that the service user is receiving similar care elsewhere, or there is sufficient and justifiable grounds to consider the service user to have lack of capacity. The care workers who are the leads for the service users care must make an assessment of the service user's capacity to provide consent. If the service user is not currently receiving care from the Care Trust the Data Protection Officer or Caldicott Guardian must be consulted.

Where the person's capacity is not sufficient to be able to make a decision with informed consent about sharing their personal information then the individual responsible for the vetting **must** override the service user's consent in giving access to the third party. **Note that the Care Trust cannot grant consent on behalf of the service user unless the Care Trust has the authority under the Mental Health Act to do so.**

If there is a capacity issue in giving informed consent, the lead care workers are obligated to reassess the capacity of the individual within a reasonable time frame so as to allow the applicant's request to be properly considered. Capacity is continually reconsidered until such time as capacity is regained and the service user can provide a decision.

5.12.3 Service User Representative's/Guardian's control over information

Some service users may have court appointed representatives or guardians (hereafter referred to as guardians) able to make decisions on the service users behalf. The Care Trust recognises the duties of the guardians but requires written proof of a guardian's ability to provide consent to access a service user's information. This proof must be submitted to the Data Protection Officer or Caldicott Guardian for authentication and no instructions from the guardian can be taken until such authentication is confirmed.

Where a guardian applies to release a service user's information to a third party or themselves (as opposed to providing consent for other people's applications), written proof of this authority and the need to provide this information must be provided to the Data Protection Officer. The Data Protection Officer has sole discretion in confirming this authority and no information should be released until the guardian's authority is confirmed.

5.12.4 Explicit Advanced Directives

Service users who have lost the ability to provide consent through any method, including death, will still have their wishes respected by the Care Trust in relation to the confidentiality of their information. Service users have the right to request the Care Trust deny third parties (specific parties or general types of parties) access to their information for. When vetting information, care must be taken to ensure that any advanced directives of the service user is recognised and communicated to the Data Protection Officer as well as the staff who are managing the release of the information. If a service user has specifically denied access to their information, the individual responsible for the vetting are to treat the information as though it is sealed (see section: Sealed information).

5.12.5 Implicit Advanced Directives

Where it is obvious to the care workers involved in the vetting process or in providing care to the service user that the service user would not have wanted their information provided to certain parties, but there are no advanced directives recorded, the Care Trust may still be able to deny access. To do this however, the individual responsible for the vetting must gather sufficient evidence and present it to the Data Protection Officer. Whilst the Data Protection Officer has sole discretion to make the decision on behalf of the Care Trust, they will be required to consult with relevant parties.

If information is to be denied release due to implicit advanced directives the individual responsible for the vetting must include the evidence of the implicit advanced directive within the associated care record.

5.13 Releasing Information as Copies

Information can be accessed through providing a copy of documents. There are considerations to releasing information this way that this section provides guidance for.

5.13.1 Responsibilities for creating and forwarding copies

The creation of copies of service user records is the responsibility of the team or service that created and/or holds the records. The costs of copying records will be held by the team or service, although in exceptional circumstances some or all of the costs may be reimbursed. Teams and services should apply to the Data Protection Officer for reimbursement.

It may also be requested that the team or service forward the copies onto the service user. If the team or service does not want to absorb the expense of forwarding the information to the applicant, it can send the records to the Information Request Office to forward to the applicant.

5.13.2 Providing appropriately to the request

Information must be supplied to applicants in accordance with their wishes. The Care Trust has, where it is reasonable to comply, a responsibility to provide information to the preference of the applicant. This includes providing information in accordance to the applicant's request of:

- Translating the information into another language.
- Preference of media (e.g. paper, electronic, Braille, audio, etc).

If considering the reasonableness of the request, this must be discussed with the Data Protection Officer.

Costs in accommodating unusual requests are carried by the team or service responsible for the information. Some costs may be charged back to the applicant however, and if this is to be a request to charge the applicant then it must be made to the Data Protection Officer who will arrange the payment.

5.13.3 Costs of creating a copy

It is appropriate to charge the applicant if there is sufficient cost in creating the copy. **All charges will be assigned and collected by the Data Protection Officer**. Charges will be the following for creating photocopies of documents:

Copies of Manual Records or Mixed Manual and Electronic Records	
Number of Pages	**Charge**
Less than 50 pages	Free
50 pages or greater	£7.50 + 15p per page after 50
Greater than 333 pages	Maximum Charge of £50.00
Copies of Electronic Records	
Number of Pages	**Charge**
Less than 50 pages	Free
50 pages or greater	£7.50 + 15p per page after 50
Greater than 67 pages	Maximum Charge of £10.00

Charges will be calculated across multiple requests within a reasonable time period of each other and on the volume of copying for each request.

The Care Trust, at the decision of an Executive Director, suspend any charge to an applicant for providing copies.

5.13.4 Considerations when creating copies

When creating copies of records the following should be considered:

- If information is removed (see section: Preparing for Release of Information), can the document have areas blanked out (i.e. create a copy, edit the copy with a black marker, then copy the copy) or does the information need to be re-made on a new document?
- Do the copies have obvious references to who created them, when they were created and where (organisation and unit) they are from? If not it would be appropriate to bind them together and provide a cover sheet to at least identify the service/team/ward they are from, the date and the primary care worker.
- Is any information missing? If information is not deliberately removed but is not present to be copied, a note should be created for the applicant stating that information would normally be available but is currently missing. The note should also say that the information will be provided should it be found.

5.13.5 Providing Information in Person

Applicants may opt to pick up their requested information straight from the Care Trust rather than having them delivered. If this is the case then the team or service who is responsible for the information must confirm the identity of the person picking up the information from them. Pick-up arrangements may need to include requesting the applicant supply identification or having a member of staff who would recognise the person verify their identity. It is appropriate to refuse to provide the information if the person's identity cannot be confirmed. Only the applicant may pickup the information, they may not send a representative without prior arrangement with the Data Protection Officer.

5.14 Releasing Information as Viewings

Information can be accessed through providing a viewing of documents. There are considerations to releasing information this way that this section provides guidance for. This guidance is appropriate and required for casual or formal viewings.

5.14.1 Responsibilities for providing viewings

The team or service responsible for the requested information is responsible for arranging the time and personnel to attend the viewing with the applicant. Costs of arranging the time and personnel remain with the team or service. The only exception to this is in the instance of

outpatient clinics consisting of singular consultants with no other supporting clinical staff. Arrangements for viewings in these instances can be made via the Data Protection Officer.

5.14.2 Requirements of a viewing

Viewings have specific requirements that must be met in order to make them possible. These are primarily relevant to the viewing of personal information by service users and take into account health and safety standards of the Care Trust*. Where health and safety standards do not already provide guidance the following must be considered:

- At least one person responsible to the Care Trust must be with the original sets of documents at all times (if the original are to be viewed).
- At least one person must be present for that applicant to be able to ask technical questions. (Technical questions are questions about the information, not about the reasons or justifications for the information. E.g. providing definitions of terminology but not answering questions of why did the doctors prescribe this drug).
- At least one person responsible to the Care Trust must be present who has qualifications for control and restraint techniques. This is particularly important if the applicant is unknown to the team or service. There should be at least one person of this type per applicant or additional unknown third party in the room.

*Note that one person could fulfil all of these roles. It is not required to have multiple staff members unless otherwise stated.

In addition it may also be wise to consider, depending on the circumstances*:

- Having a person who is a trained counsellor to assist with any distress the applicant may experience when reviewing the notes.
- Have a person who can answer questions as to the reasons for treatment present. This is not required and the Care Trust can ask for these questions to be provided for separately to the applicant's viewing of the information.
- If the applicant is female it is likely to be appropriate to only have another female member of Care Trust staff officiating the viewing, otherwise multiple members of staff should be present at all time.

*Note that one person could fulfil all of these roles. It is not required to have multiple staff members unless otherwise stated.

In terms of the environment of a viewing the following must be available:

- There is a clearly marked exit to the room that is not obstructed.
- Care Trust members of staff must be positioned in a way such that the applicant or any other third party cannot obstruct them if they wish to use the exit.
- The room should be a smoke free room.
- The room should have sufficient lighting and be a comfortable temperature.
- The applicants and any other third parties should be made aware of emergency escape routes and disabled safe havens for the site.
- The applicants and any other third party should be offered use of public rest rooms as appropriate to the site.
- No food or drink should be present such that it could damage or destroy original documents.
- If required, sufficient supplies should be available to the applicant in order for them to mark documents of interest for later copying or reference (yellow sticky pads are recommended, please avoid tape as it may damage documents when removed).

Viewings are not recommended to take place outside Care Trust sites. If this is impossible, then all similar precautions should be taken.

5.14.3 Providing appropriately to the request

In the event of a viewing the Care Trust is expected to reasonably meet the requests of the applicant in terms of:

- Special viewing equipment (e.g.: Microfiche readers).
- Translators.
- Health and Safety (e.g.: Wheelchair friendly viewing platform).
- Any other consideration required for the applicant to be able to comfortably and safely view the information.

Costs for arranging special requirements remains with the teams and services.

5.14.4 Selecting personnel in attendance for a viewing

If a viewing is to take place and the applicant is known to the Care Trust, it is the responsibility of the lead care worker to authorise the people in attendance. The lead care worker has the responsibility to assess the applicant in respect to the safety of the staff. Where the staff are unfamiliar with the applicant the lead care worker has the responsibility to brief them of any potential behaviours or risks. The lead care worker is responsible for ensuring that the requirements are met (see section: Requirements of a viewing) in terms of the staff skill sets to be in attendance.
Where the applicant is unknown to the Care Trust, the team or service must select adequately trained staff for the viewing.

5.14.5 Additional third party attendance at viewings

Third parties (those people who are not the original applicant) may only attend a viewing if they have the authority to do so or have the consent of the service user that the information is about. Third parties with the authority to view the information must provide written proof of this authority to the Data Protection Officer prior to being provided access, and must not be granted access until the team or service has received confirmation of this authority from the Data Protection Officer. Teams and Services have the obligation to deny access to the information until such confirmation has been received.

Where the third party has the consent of the service user whose information is being accessed, the team or service must first confirm the service user's capacity to provide such consent (it is advisable to do so immediately). If the service user does not have the capacity then the access to the information is to be refused for the third party only (the original applicant may still access as per normal). If the service user's capacity has been confirmed and they provided consent then the third party is to be granted access.

5.14.6 Services to be provided during a viewing

Access to information during a viewing has the only the following purposes:

- To allow the applicant to review the information.
- To allow the applicant to ask questions about what the information is
- To allow the applicant to note sections of interest for further inquiry or action

At the discretion of the Care Trust representatives the applicant may be allowed the following. If for any reason the Care Trust representatives do not wish to enter into discussion or provide the following then the applicant must make a formal written request for them to the Data Protection Officer.

- Provide justifications for the information collection or usage of the information, or the clinical decisions made.
- Provide the opportunity to make corrections or amendments.
- Make copies of the sections of interest if this was not part of the original request.

- Any discussion which is otherwise not related to the definition of the language used in the information or the education of the applicant to assist in understanding the information.

It is worthwhile noting that the applicant only has the ability to view the information requested in the initial request and cannot, unless the teams or services are happy to otherwise, expand the scope of the information to be viewed beyond what was initially agreed.

5.14.7 Length and frequency of viewings

The Care Trust is obliged to provide sufficient time for the applicant to view the records. In practicality large sets of information may take more than one viewing in order to see the entirety of the information. The Care Trust therefore can specify that the viewings will be broken into manageable sessions. The minimum session should be no less than one hour unless the volume of information to be viewed is extremely small.

Sessions must be arranged to be convenient to the applicant. The applicant must, in total of all the viewing session, be given a reasonable amount of time to review the entirety of the information.

Viewings provided on an informal basis (see section: Informal Requests) are not bound by the requirements providing sufficient time or frequencies. If the service user requires greater time or more viewings to be arranged they must make an official written request for it.

5.15. Third Party Access to Information

There are different considerations for releasing information to third parties than to the subject of the information. This section outlines how and what third parties may have access too.

5.15.1 Who are third parties?

Third parties are anyone who is not either the subject of the information or a member of the Care Trust. In some situations, particularly in the case of sealed information, other units or members of the Care Trust may be considered third parties.

A list of common third parties requesting information would include, but not be limited to:

- Police
- Local authorities
- Government
- Media
- Private companies
- Courts
- Lawyers
- Friends and Relatives
- Social Services

Only in very limited circumstances do any of the above mentioned parties have direct and unrestricted access to information. In all events of these third parties asking for information, the request must come to the Data Protection Officer or Caldicott Guardian. Third Party requests can never be granted on an informal basis.

5.15.2 Statutory Gateways for third party access to information

Some third parties have the statutory ability to access information without the consent of the subject of the information. The following list includes, but is not limited to, the more commonly encountered statutory gateways. **Under no circumstance should a member of the Care Trust make any decision to disclose information via these gateways without having it approved by the Data Protection Officer or the Caldicott Guardian first.**

- Police – Under the Data Protection Act 1998
  - Have the right to request information for the prevention, prosecution or detection of serious crimes (i.e.: crimes that can result in imprisonment).
- Social Services – Child Protection
  - Request information be provided for an assessment be made in relation to the safety/welfare of a child.

- Relatives – Under the Mental Health Act and Access to Health Records Act
  - May receive via an Approved Social Worker limited and sufficient information for their role as a carer.
  - May request under a legitimate claim to have access to the records of a deceased person.
- Courts – Under statutory rights and rights of Common Law
  - May request any information using a court order.

These gateways may be facilitated by Data Sharing Agreements. These agreements limit the amount of information released and specify to whom it may be released. If there is any question about a Data Sharing Agreement it should be directed to the Caldicott Guardian.

5.15.3 Authorisation in relation to third party requests.

In general the following positions are responsible for authorising transferring information to third parties:

- For transfer to individual members of the public, including relatives, the responsibility falls to the Data Protection Officer.
- For transfer to other organisations or institutes, including police, social services, and other NHS organisations, the responsibility falls to the Caldicott Guardian.

5.15.4 Considerations for provision of information to third parties under statutory gateways

Third parties requesting information via a statutory gateway usually limit the information to be provided. When a request comes via the authority of a statutory gateway the Data Protection Officer or the Caldicott Guardian will provide specific instructions to the vetting care worker as to what information is to be provided. Usually this will consist of specific information to answer particular questions or about a specific subject matter.

The lead care worker vetting the notes is responsible for the selection of information. Unless instructed otherwise the lead care worker must still vet the information as per normal.

5.15.5 Considerations for provision of information to third parties under consent

Third parties may have the consent of a service user to have access to their information. Where this has been granted by the service user the Care Trust must assess the service user's capacity to provide such consent (see section Consent for third parties to access information). If the consent is valid the individual responsible for the vetting must vet the information as per normal.

Note that consent for a third party to access the notes is not the same as providing consent for the third party to access the notes as though they were the service user. The consent only provides access to the notes and does not diminish the individual responsible for the vetting responsibility to protect the service user and the parties who will be accessing the notes.

5.15.6 Consent for repeated/continual access

Third parties cannot be given continual access to a service user's personal information without the explicit approval of the Data Protection Officer or the Caldicott Guardian. A request for continual access must be given to either of the above named parties for their consideration.

5.16 Further Guidance

This section provides information as to where further guidance can be found for the disclosure of personal information.

5.16.1 Care Trust resources: Data Protection Officer

The Data Protection Officer's role in the Care Trust is to ensure that the Care Trust meets its responsibilities under the Data Protection Act 1998 and the Access to Health Records Act 1990. The Data Protection Officer is available to staff and the public for:

- Providing explanation and guidance on this policy.
- Authorising and coordinating requests for information under this policy.
- Providing explanation and guidance on the Data Protection Act 1998 and Access to Health Records Act 1990.

The Data Protection Officer can be reached at:

Information Request Office
Camden and Islington Mental Health and Social Care Trust
Room 120, 1st Floor, East Wing,
St Pancras Hospital
4 St Pancras Way
London NW1 0PE

Phone: 020 7530 3019
Fax: 020 7530 3021
Email: information.request@candi.nhs.uk

5.16.2 *Care Trust resources: Caldicott Guardian*

The Caldicott Guardian's role is to ensure that the NHS Caldicott Guardian concepts are represented within the Care Trust. This includes specific principles for the release of information to organisations or institutions outside of the Care Trust. The Caldicott Guardian is available to staff and the public for:

- Providing explanation and guidance on existing Data Sharing Agreements.
- Developing and maintaining new Data Sharing Agreements.
- Providing authorisation and guidance on the disclosure of information to outside organisations/institutions outside of an existing Data Sharing Agreement.
- Coordinating, providing guidance on, and developing the Caldicott Guardian principles within the Care Trust.

The Caldicott Guardian can be reached at:

Medical Director/Caldicott Guardian
Camden and Islington Mental Health and Social Care Trust
2nd Floor, East Wing
St Pancras Hospital
4 St Pancras Way
London NW1 0PE

Phone: 020 7530 3076
Fax: 020 7530 3083

5.16.3 External Resources: Information Commissioner

The Information Commissioner is the independent official appointed by the Crown to oversee the Data Protection Act 1998. The Commissioner provides the public independent support in answering queries about the Data Protection Act and the responsibilities of public authorities, such as the Care Trust, in relation to this act. The Commissioner can also assist the Care Trust in providing expert advice in the provisioning of information under the Act. It should be noted however that the Commissioner is only able to provide advice and has no general authority to enforce its advice outside a complaints situation.
The Information Commissioner can be reached at:

Information Commissioner
Wycliffe House
Water Lane, Wilmslow
Cheshire
SK9 5AF

Phone: 01625 545 745
Fax: 01625 524 510
Email: www.informationcommissioner.gov.uk

6. 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.

The Care Trust Data Protection Officer is contactable in regards to this policy. Please contact: Timothy d'Estrube 020 7530 3019

7. EDUCATION AND TRAINING

- Self training is expected.

8. AUDIT

- There is no current audit mechanism.

9. REVIEW

Date/Trigger	Review Areas
Time Independent Reviews	
Changes to the Data Protection Act 1998	As required
Changes to the Access to Health Records Act 1998	As required
Changes in address for the Data Protection Officer or Caldicott Guardian	As required

Timed Reviews	
Post-Consultation tweaking. Expected 09/05 – 02/06	All applicable areas
Yearly Review, Sept every year	All applicable areas

10. REFERENCES

- Data Protection Act 1998 – Department of Constitution Affairs
- Access to Health Records Act 1990 - Department of Constitution Affairs
- Freedom of Information Act 2000 - Department of Constitution Affairs
- Guidance by Information Commissioner – www.ico.gov.uk

APPENDIX 1

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,