The Tavistock and Portman NHS
NHS Foundation Trust

Corporate and Directorate of Education & Training Records Procedure

Version:	2
Bodies consulted:	Caldicott Guardian, Associate Dean for Governance
Approved by:	PASC
Date Approved:	21.9.16
Lead Managers	Governance Manager
Lead Directors:	Deputy Chief Executive
Date issued:	Sep 16
Review date:	Aug 21

Contents

Corporate and Directorate of Education & Training Records Procedure

1 Introduction

The Trust recognises the importance of the creation and maintenance of its corporate records, which provide its 'corporate memory' by providing evidence of actions and decisions, and providing a key support to the daily functions and operations of the Trust.

This procedure, and associated procedures, have been drawn up in line with the Information Governance Alliance's guidance and set out how non-patient records are handled at the Trust to ensure that procedures are in place for the creation and management of authentic, reliable and usable records that will meet legal and regulatory purposes, and support the business functions and activities of the Trust.

The Trust is committed to ensuring the effective management of corporate records so that Freedom of Information and subject access requests can be efficiently responded to whilst maintaining the confidentiality and security of records.

2 Scope

This procedure is to be followed by all Trust staff, including temporary and honorary staff, who create, manage, or access corporate records in whatever format (e.g. paper, electronic, CD or other storage format).

3 Definitions

Corporate Records

These are records (in any media) that relate to, or provide evidence of, the delivery of the corporate business of the Trust. These include records generated, held and /or archived by the following functions in the Trust:

- Chief Executive's Office
- Directorate of Education and Training
- Trust Secretariat including membership
- Commercial
- Estates and Facilities

- Finance and procurement
- Informatics
- Information Communication Technology
- Clinical Governance
- Information Governance
- Human Resources
- Communications

Records

The ISO standard, ISO 15489-1:2016 Information and documentation -Records management, defines a record as 'information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business.

Specific guidance on important record types is set out in appendix 4.

Records Management

Records management relates to the systems and processes that are involved in the following activities:

- Records control, tracking and security
- Records access, retrieval and disclosure
- Records appraisal, retention and disposal
- Records storage/archiving and transfer
- Records audit/inventory and review
- Disaster preparedness and business continuity processes
- Records of training and education

4 Duties and responsibilities

6.1 Deputy Chief Executive

The Deputy Chief Executive will be responsible for assessing the assurance that this procedure has been implemented, and ensuring that any recommendations for action have been implemented.

6.2 Governance Manager

The Governance Manager is responsible to the Deputy Chief Executive for ensuring that the Trust has an effective high level procedure in place for the management of corporate records, to ensure the procedure is implemented, and to manage designated corporate records as Information Asset Owner.

The manager is responsible for creating and implementing records management tools and guidelines, and for developing, co-ordinating and monitoring records management systems and processes. The manager will provide assurance of this work by making the Trust's submission of the NHS Information Governance Toolkit compliance return to NHS Digital.

The Information Governance Lead will maintain a register of Information Asset Owners (see below).

The manager will provide performance updates and make recommendations to the Executive Management Team.

6.3 Senior Information Risk Owner

The Senior Information Risk Owner is the executive responsible for all information risks. He reports on the discharge of this responsibility through the Information Governance Work Stream of the Clinical Quality, Safety, and Governance Committee and the information processes embedded within the organisation.

6.4 Directors

Shall ensure that staff in their directorate follows this procedure for all corporate records that they create, access and/ or store. The Director will ensure that staff in their directorate cooperate in any audit activity related to corporate documents that the Trust carries out. The Director will ensure that arrangements for the management of Subject Access Requests are in place.

6.4 The Director of Education and Training

The Director is responsible for specific compliance in relation to student records in addition to his responsibility for general compliance.

6.5 Information Asset Owners

Some corporate records are also information assets, for more detail on information assets, refer to the Information Asset Acceptance and Registration Procedure.

6.6 Managers

Manager must ensure that systems are in place and staff are trained to implement this procedure. It is the manager's responsibility to ensure that inventories are kept up to date.

6.7 All Staff

All Trust staff, whether clinical or administrative, who create, receive and use records have records management responsibilities. In particular, all staff must ensure that they keep appropriate records of their work in the Trust and manage those records in keeping with this procedure and with any guidance subsequently produced. This also includes those performing temporarily in different roles. Professional staff must, in addition, comply with the directions of their professional body.

5 Procedures

7.1 Records creation, capture and maintenance

7.1.1 Creation

Staff should ensure that they formally record by all decisions and transactions made in the course of their work. This can include making file notes of telephone conversations and minutes of meetings etc.

All paper based records should be placed into an indexed and organised official file. This includes all official outgoing communications, including letters, faxes, and e-mails.

Activities and business transacted electronically, including email, also need to be captured as part of a record keeping system, and stored on a shared drive on a Trust server (not on individual PC hard drives).

7.1.2 Records Inventory

The respective manager will establish and maintain mechanisms through which their team can create an inventory of the records they are maintaining. This will be a tool called a Records Management Inventory. This inventory will benefit business processes by:

- recording of the owner and location of Trust records
- recording how records have been disposed of e.g. by destruction
- improving access to material, not just for legislative compliance, but also for internal day-to-day purposes

- providing a critical analysis tool to measure and report on Trust record keeping habits.

Advice on indexing/ numbering protocols, including the content and maintenance of Inventory records, may be sought from the Governance Manager.

7.2 Records control, tracking and security

7.2.1 Version control and reducing risks of duplication,

Appropriate access and version controls should be applied throughout records lifecycles, reflecting both legislative requirements and Trust policies. Version control helps to ensure records are fixed in time. The simplest way of doing this is through adding the version number to a footer. Version numbers for minor changes to documents should go up from Version 1.0 to 1.1 and 1.2 etc, whilst significant changes to a document should lead to a new version number e.g. 2.0.

Where possible all staff must avoid duplication and printing copies of records. This increases risks of breaches of confidentiality and needlessly increases administrative and paper costs felt by the Trust. Where the creation of copies is unavoidable, they must be destroyed as soon they are no longer needed to ensure that a version that has become obsolete is not used.

7.2.2 Tracking

This process ensures that a file can be quickly located and retrieved, particularly when stored in offsite archives.

The manager responsible for sending any files for offsite archiving must retain a schedule of the contents of the archive box in an easily accessible place to facilitate accurate retrieval. Once a file has been moved to the archive this should be recorded on the inventory.

7.2.3 Security and Storage

The security of all Trust records is critical, as records provide evidence of business transactions, support management decisions and ensure mandatory requirements are met. Records should be stored securely to prevent unauthorised access, destruction, alteration or removal.

Paper records that are sensitive, or hold confidential information, should be placed in a secure storage area when not in use. Paper records must be stored in secure and preferably alarmed facilities with strict access controls in place. Electronic records must be protected at all times from unauthorised disclosure, access and corruption.

Corporate records are not to be removed from the Trust's premises without written permission from the Governance Manager.

Records of a sensitive or personal nature must not be left unattended when not in use; this may lead to an unauthorised disclosure of information or breach of confidentiality.

7.3 Records access, retrieval and disclosure

7.3.1 Access

Records must be available to all authorised staff who require access to them for business purposes. Access to records required by contractors undertaking work for the Trust (e.g. internal audit) must be under the supervision of the manager responsible for the record.

7.3.2 Retrieval of Corporate records held electronically

All Trust electronic corporate/DET records must be stored on shared drives, which are regularly backed up, and not on personal (eg 'C:') drives or removable storage media.

This enables the faster retrieval of information by staff other than the author were appropriate and necessary; it also greatly reduces the risk of loss due to the failure of mobile devices or desktop PC hard drives.

7.3.3 Disclosure

Personal identifiable information held on corporate records must be treated as strictly confidential and may only be disclosed to individuals authorised as part of their day-to-day work to have access to it, or with the written consent of the person who is the subject of the record.

There are exceptions where disclosure is permitted, for example where under common law there is an overriding public interest or the investigation of a serious offence. The Governance Manager will be able to offer further advice where necessary.

All requests for Trust information from the public, patients, external companies, or media must be channelled through the Freedom of Information Officer.

7.4 Records Retention and Disposal

7.4.1 Retention

It is a fundamental requirement that all the Trust's corporate/business records are retained for a minimum period of time for legal, operational, research and safety reasons. The length of time for retaining records will depend on the type of record and its importance to the Trust's business functions, including any possible future litigation.

The Trust has adopted the retention periods set out in the *Records Management: NHS Code of Practice for corporate records* (the Code); this is published as the Records Retention Schedule.

Trust records must be protected, maintained, easily located and useable throughout their retention period and must be disposed of in accordance with the Code and the Records Retention and Disposal Schedule.

Convenience copies or duplicates/excerpts created from master documents by departments for local management needs or specific projects must be appropriately disposed of when they are no longer needed e.g. copies of Department of Health reports kept for information only, or duplicated sets of minutes reproduced for ready reference.

To indicate a need for consideration of further or permanent retention, an archive request form should be added to the record.

7.4.2 Disposal

Once a retention period has expired, the record must be considered for retention for:

- a further period of retention
- destruction
- transfer to a place of permanent deposit.

If there is no business need to retain the record for longer, records containing personal or confidential data must be destroyed via the Trust's confidential waste bins, other records can be disposed of in the normal way.

All Trust records held electronically, irrespective of format, are covered by the same NHS Code of Practise Retention and Destruction Schedule, and therefore can be deleted when the retention period has passed.

7.5 Vital Records and Business Continuity

Vital Records are those records without which an organisation could not continue to operate. They are the records which contain information needed to re-establish the business of the organisation in the event of a disaster or significant interruption to business and which protect the assets and interests of the organisation.

The Trust must protect these Vital Records by putting in place controls that protect their existence and ensure their availability should they ever be needed. In order to do so the Trust will:

- identify critical processes and functions
- identify key internal and external dependencies on which these processes rely
- identify the records relating to the critical processes and functions
- make sure all departments identify, record, and protect their vital records.

Examples of records which might be classified as vital are:

- Trust Board and assurance committees
- Minutes of Executive Management Team meetings
- Manuals and instructions
- Pay rates and other personnel records
- Annual reports
- Legal documents, including current contracts
- Computer software programmes and data
- Accounts, payable and receivable
- Contracts and formal agreements
- Contact information for key staff
- Indexes/finding aids to records.

There are three main options for protecting Vital Records and the Trust requires that at least one of these must be used for each type of documents

- Retention in an electronic format on servers
- Duplication and dispersal (the duplicate may be in paper or alternative format, such as microform or CD,) -records on Trust servers are automatically duplicated
- Use of fireproof and secure storage facilities
- Remote storage.

Vital Records should be stored in protective or fire resistant conditions with suitable access conditions; confidential records should be stored in locked metal storage cabinets.

The storage of records in electronic form may involve significant risks but many of these can be avoided by the use of adequate storage plans and strategies. A back-up system is required and this should be set out in the respective business continuity plan.

7.6 Auditing Corporate Records

The Governance Manager will carry out audits of corporate records to establish:

- the types of records held
- form of records held
- whether records are managed in line with the procedures above

The Trust audit template and smart action plan *pro forma* (Appendix 1) will be used to report the findings and action plan following each audit.

7.7 Responding to requests from individuals for access to records

All staff need to be aware that there is a legal right to request access to personal information; such requests must promptly be passed to an appropriate person in the respective directorate. Requests for access to health records are dealt with under the Health Records Procedure, which follows a similar process.

Under the Data Protection Act 1998, an individual who makes a request for access to personal information held by the Trust is entitled:

- to be told whether their personal information is being processed by the Trust or someone else acting on its behalf and if so, to be given a description of:
    - the personal information;
    - the purpose for which the information is being processed, and
    - those to whom it is or may be disclosed.

- to be told in a way they can understand:
    - the information which constitutes the personal information; and
    - the source of the information (the Trust is not obliged to disclose such information where the source of the information is, or can be identified as an individual, without that person's consent unless it is believed to be reasonable to do so).

The Access to Records Process is detailed in appendix 3. General enquiries are handled through the office of the Governance Manager who will refer the request to the respective department.

7.8 Right of Appeal

The Data Protection Act 1998 provides an avenue of appeal to the Information Commissioner about any decisions to refuse access to records. This right can be exercised in cases where rights of access have been refused on the ground that another person who has supplied information has not consented to its disclosure, where this would identify him or her, or where that person cannot be found in order for their consent to be sought. In the light of this right it is vital that any decision to withhold information is documented with detailed reasons, so that if necessary an explanation/defence to any enquiries can be prepared.

7.9 Repeat Requests for Access

A response to an access request does not have to be made if it is made very soon after an identical or similar previous request. In deciding whether it is too soon, consider the type of information, the purpose(s) for holding it, and how often it changes are matters to be considered before access is granted.

7.10 Exemptions

Exemptions from the subject information provisions and the disclosure provisions of the Data Protection Act 1998 may be available in the following circumstances:

7.10.1 Prevention or Detection of Crime

The data subject need not be informed:

- that an organisation is holding personal information about him/her for the purposes of the prevention of crime;
- that an organisation is holding personal information about him/her to apprehend or prosecute offenders;
- that information about him/her has been disclosed to another organisation which required it for any of these purposes (e.g. the police);
- that it received information from an organisation which had it in its possession for any of these purposes;
- that it is holding personal information about him/her if the provision of such information would be likely to prejudice such disclosure or would be likely to prejudice any of these purposes.

(Requests should be treated on a case by case basis and use of the exemption should be the exception rather than the rule. Legal advice may be sought by the Governance Manager where doubt exists.)

7.10.2 Disclosure Would Cause Physical and/or Mental Harm

Access shall not be given to any part of the record which the Trust representative feels would disclose:

either information likely to cause serious harm to the physical or mental health of the data subject or of any other individual

or information relating to or provided by an individual other than the data subject, who could be identified from that information.

The above does not apply if other identifiable individuals mentioned in the record or providing information in the records consent to the application for access or the individual is a health professional who has been involved in the care of the patient.

Staff have a common law duty of care to all parties. There may be situations where information is withheld as disclosure to the data subject would be likely to cause serious harm to the physical or mental health, or condition, of the subject or another person. (Restriction on the right of access should be exceptional and confined to serious harm, for instance, where there is sufficient risk to the safety of a child for a child protection plan to be in place and where disclosure would prejudice the plan.)

6 Training Requirements

The Trust is committed to ensuring that staff retain a sound grounding in information Governance and safe records management and therefore have adopted the recommendation that all staff will complete an IG training programme (full programme or update annually as part of the manual training programme). Compliance will be monitored at the Executive Management Team.

7 Process for monitoring compliance with this Procedure

Operational compliance will be monitored at team level by the respective manager who shall undertake spot checks. The Trust's performance overall will be reported termly by the Governance Manager as part of the IG Update.

The results of the audits will be considered by the Information Governance work stream and reported by exception to the Clinical Quality, Safety, and Governance Committee giving assurance that evidence has been received that has been deemed to show compliance with this procedure, or where compliance was not found, that credible action plans had been put in place that would generate the required evidence within agreed timescale.

8 References

http://systems.hscic.gov.uk/infogov/codes/cop

http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=62542

ICO Code of Practice
http://www.ico.org.uk/for_organisations/data_protection/~/media/documents/library/Data_Protection/Detailed_specialist_guides/subject-access-code-of-practice.PDF

Higher Education Business Classification Scheme and Records Retention Schedules - http://www.jisc.ac.uk/guides/research-data-management

9 Associated documents[1]

Data Protection Procedure
Business Continuity Procedure
Records Retention and Disposal Schedule
Data Quality Accuracy and Validation Procedure
Health records procedure
Information Governance Policy
Risk Management Strategy and Policy
ICT Security Procedure
Information Asset Acceptance and Registration Procedure
Development and Management of Policy and Procedural Documents Procedure
Selection of Records for Permanent Retention Procedure

[1] For the current version of Trust procedures, please refer to the intranet.

Appendix A : Equality Analysis

Completed by	Jonathan McKee
Position	Deputy SIRO and Governance Manager
Date	22.9.16

The following questions determine whether analysis is needed	**Yes**	**No**
Is it likely to affect people with particular protected characteristics differently?		x
Is it a major policy, significantly affecting how Trust services are delivered?	x	
Will the policy have a significant effect on how partner organisations operate in terms of equality?		x
Does the policy relate to functions that have been identified through engagement as being important to people with particular protected characteristics?		x
Does the policy relate to an area with known inequalities?		x
Does the policy relate to any equality objectives that have been set by the Trust?		x
Other?		x

If the answer to *all* of these questions was no, then the assessment is complete.

If the answer to *any* of the questions was yes, then the following analysis will provide further scrutiny:

	Yes	**No**	**Comment**
Do policy outcomes and service take-up differ between people with different protected characteristics?			
What are the key findings of any engagement you have undertaken?			
If there is a greater effect on one group, is that consistent with the policy			

aims?			
If the policy has negative effects on people sharing particular characteristics, what steps can be taken to mitigate these effects?			
Will the policy deliver practical benefits for certain groups?			
Does the policy miss opportunities to advance equality of opportunity and foster good relations?			
Do other policies need to change to enable this policy to be effective?			
Additional comments			

If one or more answers are yes, then the policy may unlawful under the Equality Act 2010 – seek advice from Human Resources (for staff related policies) or the Trust's Equalities Lead (for all other policies).

Appendix B

Tavistock and Portman NHS Foundation Trust Audit Report *Pro forma*

Services audited		
Background		
Aims and Objectives of the audit	**Aim** **Objectives**	
Methodology and Standards	**Methodology** **Standard Measured**:	
Details of data collection *(sample etc)*		
Key Results *Main results arising from the project*		
Recommendations summary *(where relevant these should be addressed on the action plan below)*		
Feedback Findings		
Acknowledgements		
Contact		Date Report

Trust Action Plan Template

When developing your action plan aim to ensure that it meets the following 5 criteria ie that it is **S.M.A.R.T.**

Specific *describe the goal that you the plan is addressing clearly and unambiguously*

Measurable *Set measures of success which may be a single target or milestones*

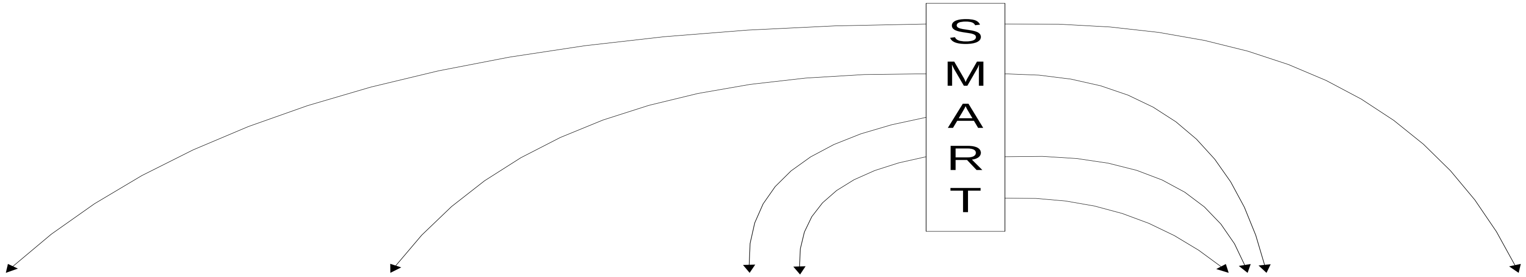
Achievable *check that the plan is achievable within available resources (if not either change the plan or develop a business case for further resources)*

Realistic *will the action plan be achievable in practice,(eg check if requires cooperation of others)*

Time-limited *set target completion date and review progress to assess progress*

Action Plan Template

The Tavistock and Portman NHS
NHS Foundation Trust



Recommendation from audit findings In ***relation to audit what recommendation are you addressing?***	**Success criteria** ***What measures*** *of success will be used to determine that the objective has been delivered*	**Plan** *Explain* ***how*** *the success criteria will be* ***achieved*** *–eg outline a* ***realistic*** *project plan, and who will monitor progress*	**Timescale** ***When*** *the plan will be delivered, as a whole or by individual success criteria*	**Lead** ***Specify who*** *is responsible*

Appendix C : How to Respond to Subject Access Requests

For access to health records, see the Health Records Procedure, all other requests should be dealt with as follows:-

Background and Introduction

This procedure provides direction to staff about the provision of access to records for data subjects and their representatives. This procedure has been written in line with the ICO guidance on subject access. Subjects have a right to the information in their records, which is not the same as having the right to a copy of their records.

1.0 Receipt of the request for Disclosure

1.1 All requests will be handled by an administrator nominated by the director of the department holding the information. If information is held in several departments then the Governance Manager will lead the management of the request.

1.2 All requests must be received in writing signed by the applicant, a legally appointed representative of the applicant, or in the case of a child, by someone who holds parental responsibility for the child.

2.0 Verification of the identity of the data subject

2.1 The Trust has a legal obligation to ensure that it does not breach any data subjects' confidentiality all reasonable steps must be taken to ascertain the identity of the data subject to ensure only the relevant information is disclosed.

2.2 The data subject, or his legally appointed representative, will be asked to provide information to enable the trust to correctly identify the relevant records this will include;

- Name of subject
- Date of birth
- Address registered at the time of contact
- Identifying number (eg HR, student)
- Name of staff contact

2.3 **Verification of Identity**

The requestor will be required to provide evidence of their identity (and evidence of their authority to request disclosure if not the data subject)

List A
Requestors will be asked to supply a copy of one of the following to support their application:

- Valid passport
- UK/EEA/EU photo driving licence. Driving licences that do not have a photo are not acceptable

- EU/EEA National Identity Card
- Northern Ireland Voters Card (with photograph)
- Firearms or shotgun licence (with photograph)

List B
If the requestor cannot provide one of the above, they will be required to supply two documents from list B:

- Benefits or State pension notification letter
- Current UK non-photo driving licence
- Blue disabled drivers pass
- All other current signed passports with valid UK Visa not listed above
- UK Birth Certificate (under 18s only)
- National Insurance Card (under 18s only)
- Medical Card/Certificate (under 18s only)

2.4 Verification of Address

List C
The requestor will be required to provide evidence of current address in the form of a photocopy of one of the following:

- Bank, Building Society or Credit Union statement (we do not accept statements printed off the internet)
- Current UK non-photo driving licence (only if it is not been used as proof of identification)
- Utility Bill/Utility Statement or Certificate/Letter from a supplier of utilities dated within the last 3 months
- Local authority tax bill/council tax bill for current year
- Benefits or pensions notification letter confirming the right to benefit (only if it has not been used as proof of identification)

Prospective requests will not be accepted until the Trust has satisfied itself as to the identity of the requestor.

3.0 **Confirmation of authority for those acting on behalf of others**

In addition to the information required in section (a) above, those acting on behalf of others will also need to supply written authority from the prospective subject, or an explanation of the circumstances why this is not possible (e.g. parent of a child) , and proof of their identity. Requests received from statutory agencies (e.g. the police or HMRC) or a personal representative (e.g. solicitors) only need be accompanied by a signed letter of authority (or form 3022 for the Metropolitan Police) to disclose.

4.0 Details of what is being requested

In addition to verifying identity the administrator should liaise with the requestor to find out which records they are requesting (however the requestor is not legally obliged to tell us the reason for their request):-

- Why the information is being requested
- Approximately when they had contact with the Trust
- Which department may hold the information.

5.0 Process for providing access

5.1 Details of the request are sent by the administrator to the relevant manager who should review the record and seek advice from the Governance Manager on disclosure.

5.2 If there may be grounds for withholding all or part of the record (see section 6 below), if so, the manager should consult with the Governance Manager.

5.3 The administrator will advise on the format of information to be supplied, e.g. whether photocopies are made or whether the information could be supplied in a different format.

6.0 **Grounds for withholding access**

Before information is released the manager should ensure that they have checked the record and considered if allowing access would result in either of the following:

- Could result in serious harm to the physical or mental health condition of the requestor, or of any other person.

  or

- Would disclose information relating to, or provided by a third person (not a health professional), who had not consented to that disclosure.

If either of these applies then the Trust may deny or limit access to the record (though this would be exceptional).

In addition, if the application is for access to a deceased person's record and the record contains information that the deceased person expected to remain confidential then it must remain so.

There is no legal obligation to advise applicants of the grounds on which information has been withheld and, if the fact that all or part of the records are withheld may cause distress to the applicant, there is no obligation to notify the applicant that records have been withheld.

7.0 Responding

7.1 The Trust has a maximum of 40 days in which to respond to requests; this time starts when the requirements in sections 2, 3, and 4 have been satisfied.

7.2 If disclosure is agreed the administrator should arrange photocopy and dispatch of the records, which must be sent recorded/special delivery, or be collected in person from the Trust.

8.0 Access Log

A log will be kept by the administrator to record how the Trust is complying with the request. A copy of the log will be submitted to the Director of Corporate Governance and Facilities at the end of each quarter.

9 Fees

The Trust may charge fees to data subjects who request access to their records. If a request comes via a solicitor then fees are generally charged at the rate set by the Director of Corporate Governance and Facilities.

Fees (correct at July 2013)

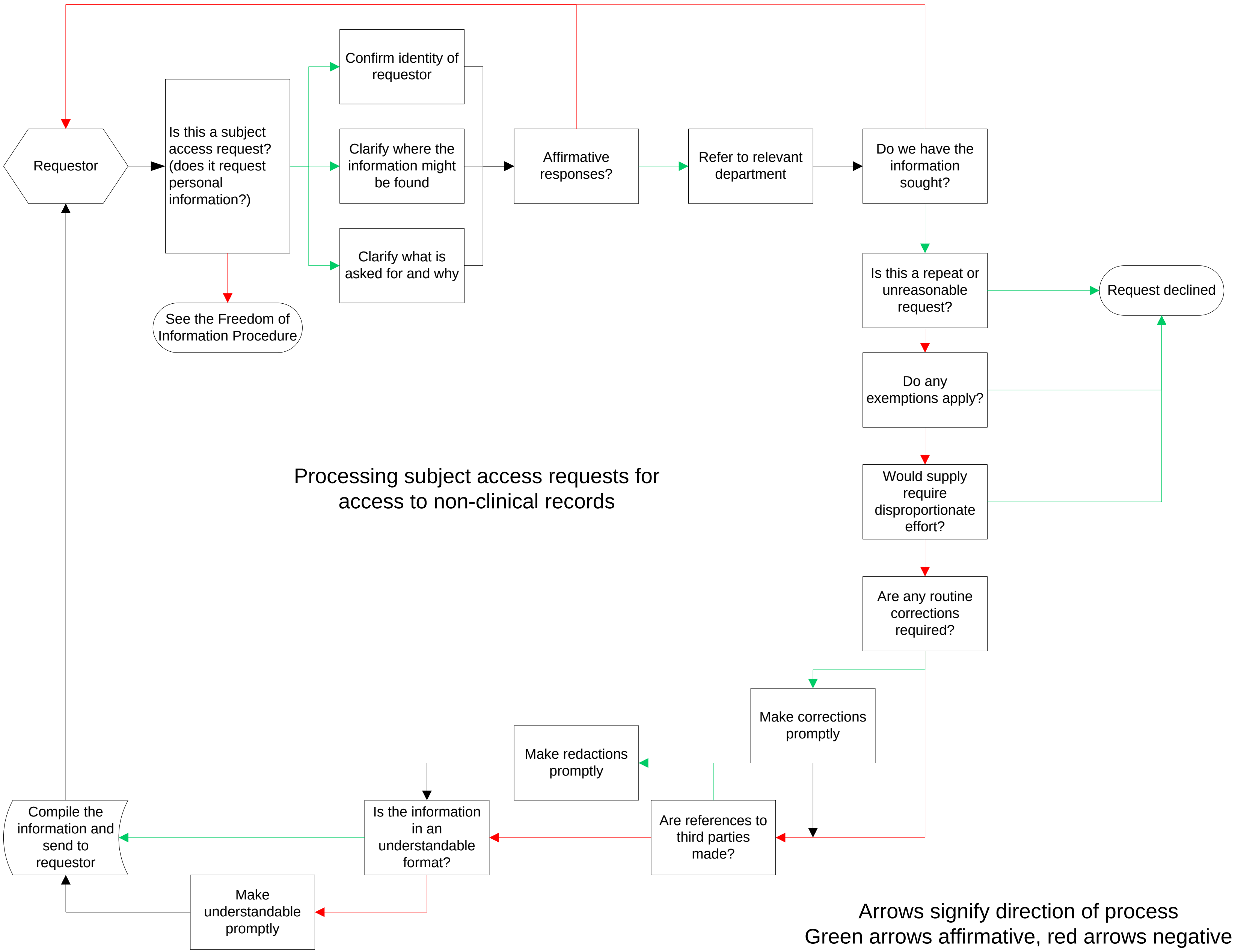
Where a copy of the record is requested:

> *Records held totally on computer: A minimum charge of £2 should be charged with copies of up to A4 size charged at ten pence a copy, plus postage costs of bulky items, up to a total maximum £10 charge.*
>
> *Records held in part on computer and in part manually: A minimum charge of £2 should be charged with copies of up to A4 size charged at ten pence a copy, plus postage costs of bulky items, up to a total maximum £50 charge.*
>
> *Records held totally manually: A minimum charge of £2 should be charged with copies of up to A4 size charged at ten pence a copy, plus postage costs of bulky items, up to a total maximum £50 charge.*
>
> *Note: These maximum charges include copying, postage and packing costs.*

8.0 Correcting a Record

8.1 If, after accessing the record, the subject feels that information recorded on their record is incorrect then they should be advised to set out what correction they would like to see made. Routine updates and corrections should be made as soon as possible. If the matter is not resolved they should be advised of the current complaints policy and procedure as outlined in the Complaints Procedure.

8.2 Statements of professional opinion cannot be changed; the subject is allowed to include a statement in their record that they disagree with specific parts of their record. The data subject could further complain to the Information Commissioner, who may rule that any erroneous information is rectified, blocked, erased or destroyed, and they may seek legal independent advice to pursue their complaint.


Requestor
Is this a subject access request? (does it request personal information?)
See the Freedom of Information Procedure
Confirm identity of requestor
Clarify where the information might be found
Clarify what is asked for and why
Affirmative responses?
Refer to relevant department
Do we have the information sought?
Is this a repeat or unreasonable request?
Request declined
Do any exemptions apply?
Would supply require disproportionate effort?
Are any routine corrections required?
Make corrections promptly
Are references to third parties made?
Make redactions promptly
Is the information in an understandable format?
Make understandable promptly
Compile the information and send to requestor

Processing subject access requests for access to non-clinical records

Arrows signify direction of process
Green arrows affirmative, red arrows negative

Appendix D : Specific guidance for important records and related processes

Complaints Records

Where a patient or client complains about a service, these are kept in a separate file relating to the complaint and subsequent investigation. Complaint information should never be recorded in the clinical record. A complaint may be unfounded or involve third parties and the inclusion of that information in the clinical record will mean that the information will be preserved for the life of the record and could cause detrimental prejudice to the relationship between the patient and the health care team.

Where multiple teams are involved in the complaint handling, all the associated records are amalgamated to form a single complaint record.

Continuing Care Decisions Records

In order to process applications and appeals for funding continuing care, it is necessary for the relevant organisation to have access to clinical records. This will be based on consent and organisations need to have arrangements in place to facilitate sharing or put systems in place to allow access to view records or take copies. Any access must be lawful and the decision to grant access recorded.

Records of Funding

Funding records are primarily administrative records but they contain large amounts of care information so must be managed as clinical records for their access and management.

Adopted Persons Health Records

Notwithstanding any other centrally issued guidance by the DH or Department for Education, the records of adopted persons can only be placed under a new last name when an adoption order has been granted. Before an adoption order is granted, an alias may be used, but more commonly the birth names are used. Depending on the circumstances of the adoption there may be a need to protect from disclosure any information about a third party. Additional checks before any disclosure of adoption documentation are recommended because of the heightened risk of accidental disclosure. It is important that any new records, if created, contain sufficient information to allow for a continuity of care. At present the GP would initiate any change of NHS number or identity if it was considered appropriate to do so, following the adoption.

Health Records of Transgender Persons

A patient can request that their gender be changed in a record by a statutory declaration, but this does not give them the same rights as those that can be made by the Gender Recognition Act 2004. The formal legal process (as defined in the Gender Recognition Act 2004) is that a Gender Reassignment Certificate is issued by a Gender Reassignment Panel. At this time a new NHS number can be issued and a new record can be created, if it is the wish of the patient. It is important to discuss with the patient what records are moved into the new record and to discuss how to link any records held in any other institutions with the new record.

Witness Protection Health Records

Where a record is that of someone known to be under a witness protection scheme, the record must be subject to greater security and confidentiality. It may become apparent (such as via accidental disclosure) that the records are those of a person under the protection of the Courts for the purposes of identity. The right to anonymity extends to medical records. For people under certain types of witness protection, the patient will be given a new name and NHS Number, so the records may appear to be that of a different person.

Occupational Health Records

Occupational health records are not part of the main staff record and for reasons of confidentiality they are held separately. However, reports or summaries may be held in the main staff record where these have been requested by the employer and agreed by the staff member. When occupational health records are outsourced, the organisation must ensure that any contractor can retain the records for the necessary period after the termination of service for purposes of adequately recording any work based health issues.

Staff Records

Staff records should hold sufficient information about a staff member for decisions to be made about employment matters. The nucleus of any staff file will be the paperwork collected through the recruitment process and this will include the job advert, application form, right to work, identity checks and any correspondence relating to acceptance of the contract. The central file must be the repository for this information.

It is common practice for the line manager to hold staff records which can contain large portions of an employee's employment history (for example training records). This practice runs the risk of much of the employment record being lost if there is an internal move of the employee or upon termination of contact. It is important that there is a single record of the employment of an employee.

Upon termination of contract, records must be held up to and beyond their statutory retirement age. Staff records may be retained beyond 20 years if they continue to be required for NHS business purposes, in accordance with Retention Instrument 122. They are not exempt from Principle 5 of the DPA.

To reduce the burden of storage and for reasons of confidentiality it is recommended that a summary be prepared and held until the employee's 75th birthday or 6 years after leaving, whichever is the longer, and then reviewed.

Where a summary is made it must contain as a minimum:

- A summary of the employment history with dates
- Pension information including eligibility
- Any work related injury
- Any exposure to asbestos, radiation and other chemicals which may cause illness in later life
- Professional training history and professional qualifications related to the delivery of care

- List of buildings where the member of staff worked and the dates worked in each location

Disciplinary case files can be held in a separate file so they can be expired at the appropriate time and do not clutter up the main file. That does not mean that there should be no record that the disciplinary process has been engaged in the main record.

Email and Record Keeping Implications

Email has the benefit of fixing information in time and assigning the action to an individual, which are two of the most important characteristics of an authentic record. A common problem with email is that it is rarely saved in the business context, which is the third characteristic to achieve an authentic record. The correct place to store email is in the record keeping system according to the business classification scheme or file plan activity to which it relates. Solutions such as email archiving and ever larger mailbox quotas do not encourage staff to meet the standard of storing email in the correct business context and to declare the email as a record.

Where email archiving solutions are of benefit is as a backup, or to identify key individuals where their entire email correspondence can be preserved as a public record. Where email is declared as a record or a as a component of a record, the entire email must be kept including attachments so the record remains integral – for example an email approving a business case must be saved with business case file. All staff need to be adequately trained in required email storage and organisations need to undertake periodic audits of working practice to identify and address poor practice.

Automatic deletion of email as a business rule may constitute an offence under Section 77 of the FOIA where it is subject to a request for information even if the destruction is by automatic rule. The Courts' civil procedure rules 31(B) also require that a legal hold is placed on any information including email when an organisation enters into litigation.

Legal holds can take many forms and records cannot be destroyed if there is a known process or an expectation that records will be needed for a future legal process. This may include national or local enquiries, criminal investigation, and expected cases of litigation or records that maybe requested under FOI or subject access. This means that no record can be destroyed by a purely automated process without some form of review whether at aggregated or individual level for continued retention or transfer to a place of deposit.

The NHS mail system allows a single email account for every staff member that can follow the individual through the course of their career. When staff transfer from one NHS organisation to another NHS organisation, they must ensure that no sensitive personal data relating to the former organisation is transferred.

It is good practice for staff to purge their email accounts of information upon transfer to prevent a breach of confidence or the transfer of security classified information. This is facilitated by staff storing only those that need to be retained on an ongoing basis. Emails that are the sole record of an event or issue, for example an exchange between a clinician and a patient, should be copied in to the relevant clinical record rather than being simply deleted.

Records Created via Social Media

Where social media is used as a means of communicating information for business purposes or it is a means of interacting with clients, it may be a record that needs to be kept. Where this is the case, information must be retained within the record keeping system. This may not necessarily mean that the social media must be captured but rather the information of the activity through transcription or periodic storage.

Cloud Based Records

Use of cloud based solutions for health and social care are increasingly being considered as an alternative to managing large networks and infrastructure. Before any cloud based solution is implemented there are a number of records considerations that must be addressed. The ICO has guidance on cloud storage, they also advise to conduct a privacy impact assessment for any potential solutions.

The NHS has a prohibition on storing patient identifiable data outside of England where there is a link to national systems or applications (e.g. N3 or NHSmail), so any solution must have servers that can be traced to England if it is going to be used to store patient data.

Another important consideration is that at some point the service provider or solution will change and it will be necessary to migrate all of the records, including all the formats, onto another solution and this may be technically challenging.

Records in cloud storage must be managed just as records must be in any other environment and the temptation to use ever increasing storage instead of good records management will not meet the records management recommendations of this code.

Where personal data is stored there is also the risk of breaching the requirements of the DPA not to store personal information longer than necessary.

Website as a Business Record

As people interact with their public services, more commonly it is the internet and websites in particular that provide information, just as posters, publications and leaflets once did exclusively.

A person's behaviour may be a result of interaction with a website and it is considered part of the record of the activity. For this reason, websites form part of the record keeping system and must be preserved. It is also important to know what material was present on the website as this material is considered to have been published. Therefore, the frequency of capture must be adequate, or some other method to recreate what the website or intranet visitor viewed. It may be possible to arrange regular trawls of the site with the relevant place of deposit, but given the complexity of sites as digital objects, it may be necessary to use other methods of capture to ensure that this creates a formal record.

The UK Government Web Archive (part of TNA) undertook two central trawls of all NHS sites in 2011 and 2012 and may have captured some from 2004 onwards, but the information captured will not include all levels of the sites or some dynamic content.

Scanned Records

This section applies to health and care records as much as it does to corporate records.

Where scanning is used, the man consideration is that the information can perform the same function as the paper counterpart did and like any evidence, scanned records can be challenged in a court. This is unlikely to be a problem provided it ca be demonstrated that the scan is an authentic record and there are technical and organisational means to ensure the scanned records maintain their integrity, authenticity and usability as records, for the duration of the relevant retention period.

If this is a record type which must or may be selected and transferred to a place of deposit, the place of deposit should be asked whether they wish to preserve the hard copy and/or the scans. If the hard copy is retained, this will constitute 'best available evidence' for legal purposes, rather than the scanned copy.

The legal admissibility of scanned records, as with any digital information, is determined by how it can be shown that it is an authentic record. An indication of how the courts will interpret evidence can be found in the civil procedure rules and the court will decide if a record, either paper or electronic, can be admissible as evidence.

The standard, 'BS 10008 Electronic Information Management – Ensuring the authenticity and integrity of electronic information', specifies the method of ensuring that electronic information remains authentic. The standard deals with both 'born digital' and scanned records. The best way to ensure that records are scanned to the appropriate standard is to use a supplier or service that meets the standard. It is expected that all large scale digitisation projects will receive assistance from industry experts to ensure that the records are scanned to standard.

For small scale scanning requirements or those records where there is a low risk of being required to prove their authenticity, organisations may decide to do their own scanning.

Once scanned records have been digitised and the appropriate quality checks completed, it will then be possible to destroy the paper original. A scan of not less than 300 dots per inch (or 118 dots per centimetre) as a minimum is recommended for most records although this may drop if clear printed text is being scanned.

Methods used to ensure that scanned records can be considered authentic are:

- A written procedure outlining the process to scan, quality check and any destruction process for the paper record
- Evidence that the process has been followed
- An audit trail or secure system that can show that no alterations have been made to the record after the point they have been digitised
- Fix the scan into a file format that cannot be edited such as Portable Document Format (PDF).

Before you begin scanning, check that those for whom you may have to produce records for will accept an authentic copy. Some common mistakes occur in scanning by:

- Only scanning one side and not scanning both sides, including blank pages
- Scanning a copy of a copy leading to a degraded image
- Not using a method that can show that the scanned record has not been altered after it has been scanned
- Not having a long term plan to enable the digitised records to be stored or accessed over the period of their retention.