This document is uncontrolled once printed.

Please refer to the Trusts Intranet site (Procedural Documents) for the most up to date version

# CORPORATE DOCUMENTATION MANAGEMENT (INFORMATION LIFECYCLE)

## NGH-PO-123

| | |
|---|---|
| Ratified By: | Procedural Documents Group |
| Date Ratified: | June 2015 |
| Version No: | 3 |
| Supercedes Document No: | 2 |
| Previous versions ratified by (group & date): | Procedural Documents Group |
| Date(s) Reviewed: | June 2015 |
| Next Review Date: | June 2018 |
| Responsibility for Review: | IG Manager |
| Contributors: | IG Manager |

POLICY

**CONTENTS**



POLICY

**Version Control Summary**

| Version | Date | Author | Status | Comment |
|---|---|---|---|---|
| 1.6 | January 2007 | Gwenneth McConnell – Freedom of Information Manager | Final | New document |
| 1.7 | July 2013 | Lolu Adeniji – Information Governance Manager | Draft | Revised to align with the new Department of Health Records Management Code of Practice |
| 1.8 | August 2013 | Lolu Adeniji | Draft | Changes made to reflect comments from members of the IG Leads Board |
| 1.9 | January 2014 | Kehinde Okesola – Information Governance Manager | Draft | Review and transfer to new Trust policy template |
| 1.10 | February 2014 | Kehinde Okesola – Information Governance Manager | Draft | Changes made to reflect comments from members of the IG Leads Board |
| 1.11 | March 2014 | Kehinde Okesola – Information Governance Manager | Draft | Changes made to reflect comments from members of the Governance Team |
| 2 | March 2014 | Kehinde Okesola – Information Governance Manager | Ratified | Ratification |
| 3 | January 2015 | Kehinde Okesola – Information Governance Manager | Draft | Retention schedule update and inclusion of Appendix 2: Protective Marking Scheme to reflect the new Government Classification scheme, published April 2014 |
| 3.1 | June 2015 | Kehinde Okesola – Information Governance Manager | Ratified | Chair approved |

**SUMMARY**

This policy offers an effective documentation management function ensuring that information is properly managed and is available whenever and wherever there is a justified need for that information, and in whatever media it is required. It provides clarity on the Trust's legal obligation in the handling, retaining and destroying of corporate documentation

THE FIVE PHASES OF THE INFORMATION LIFECYCLE

This policy documents the intent of the Trust to manage ALL of its recorded information assets appropriately in accordance with the concept of information lifecycle management and throughout the five distinct phases of the documentation/information lifecycle [Fig.1]:

1. Creation

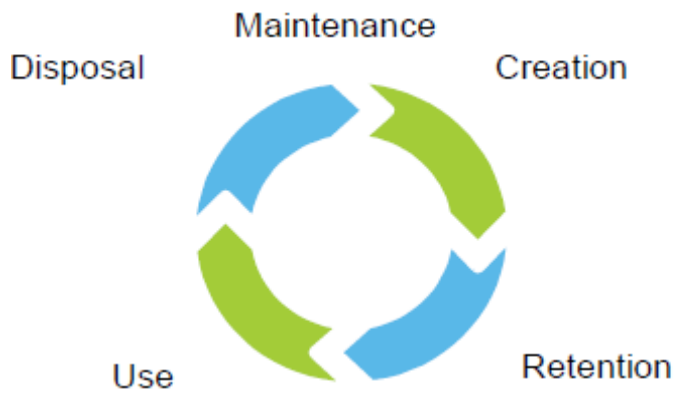
2. Retention (organisation, storage, security, etc.). Note the length of retention varies depending on the information. (Appendix 1)

3. Maintenance

4. Use (retrieval, access levels etc.)

5. Disposal (timely, with appropriate and secure media destruction methods used)

Fig.1



## 1. INTRODUCTION

The effective management of all recorded information across Northampton General Hospital NHS Trust (here after referred to as the 'Trust') is essential to operate efficiently. Within a framework of legislative compliance and best practice, non-health (business and corporate) documentation management is a core obligation for the Trust.

The lifecycle of a document refers to the life of that document from its creation/receipt, throughout its active use, access to the record, transportation of the record, its retirement to archive or preservation, the period of its retention and, its final disposal and destruction.

Documentation are a valuable resource because of the information they contain. Annually the Trust creates millions of documentation as part of our day-to-day business. High quality information underpins the delivery of high quality health care and many other key service deliverables. Managing this information to agreed standards as it is created (and throughout its lifecycle) is essential. Information is of greatest value when it is accurate and up to date. An effective documentation management service ensures that information is properly managed and available when needed

The Trust documentation are admissible as evidence in legal proceedings and must be maintained to the highest standards. Each member of staff is accountable for the documentation they create, use, transport, share, archive, or destroy.

## 2. PURPOSE

The purpose of this policy is to ensure a consistent and effective approach to the management of all documentation within the Trust by:

- Defining the role of documentation management within the Trust
- Identifying roles and responsibilities for documentation management
- Providing guidance on meeting legal and professional requirements for documentation management
- Detailing the standard to be followed for the transportation, transmission and secure storage of documentation; especially where these documentation contain person identifiable information (PID).
- Setting out Trust retention periods for all types of documentation
- Indicating how compliance with this policy will be monitored and maintained

## 3. SCOPE

This policy applies to everyone working at Northampton General Hospital NHS Trust who has any interaction with documentation, including, but not limited to, permanent staff, temporary staff, students, locums, volunteers, researchers and staff on honorary contracts (all referred to as 'staff' in this document).

For the purpose of this policy, documentation are defined as: recorded information irrespective of format, which is created, received and maintained by the Trust in the execution of its business.

This policy covers all documentation, in all formats, both active and inactive, held for use in NGH, including but not limited to:

- Non-clinical e.g. administrative, corporate, personnel, estates, finance and litigation, including emails and text messages

This policy excludes all documentation created by other organisations, such as the Department of Health, which are kept for reference and information only, unless they include person identifiable information.

It is important to note that this policy does not replace any existing policies, but works in conjunction with them where indicated. It provides a high-level overview, which sets out the connections between the various Trust policies that contribute towards the management of all Trust documentation of staff, its departments, business operations and activities.

## 4. COMPLIANCE STATEMENTS

### Equality & Diversity

This policy has been designed to support the Trust's effort to promote Equality and Human Rights in the work place and has been assessed for any adverse impact using the Trust's Equality Impact assessment tool as required by the Trust's Equality and Human Rights Strategy. It is considered to be compliant with equality legislation and to uphold the implementation of Equality and Human Rights in practice.

### NHS Constitution

The contents of this document incorporates the NHS Constitution and sets out the rights, to which, where applicable, patients, public and staff are entitled, and pledges which the NHS is committed to achieve, together with the responsibilities which, where applicable, public, patients and staff owe to one another. The foundation of this document is based on the Principals and Values of the NHS along with the Vision and Values of Northampton General Hospital NHS Trust.

The Trust will take responsibilities as necessary to comply with the professional and legal obligations set out in the Department of Health Records Management Code of Practice, as well as for ensuring compliance of associated areas including:

- The Public Records Act (1958), (1969), (1995)
- Data Protection Act 1998
- Common Law of Duty and Confidentiality
- Freedom of Information Act 2000 and Environmental Information Regulations 2004
- Secretary of State for Constitutional Affairs' Code of Practice on the discharge of public authorities' functions under Part I of the Freedom of Information Act 2000 published 2004.
- Health Service Circular 1999/053: Managing Records in NHS Trusts and Health Authorities

## 5. Definitions

| | |
|---|---|
| Documentation / Documents | 'Documentation, non-medical records and information, in any form, created or received and maintained by the Trust in the transaction of its business or conduct of affairs and kept as evidence of such activity'. |
| IG Toolkit | Information Governance Toolkit |
| FOIA | Freedom of Information (Act) 2000 |

## 6. ROLES & RESPONSIBILITIES

| ROLE | RESPONSIBILITY |
|---|---|
| **Chief Executive and the Trust Board** | Chief Executive and Trust Board have ultimate accountability for actions and inactions in relation to this policy |
| **Caldicott Guardian** | The Caldicott Guardian is responsible for ensuring the Caldicott principles are followed and that patient interests are maintained regarding holding, obtaining, recording, using and sharing their information.<br>The Caldicott Guardian for the Trust is the Medical Director. |
| **Senior Information Risk Owner (SIRO)** | The Senior Information Risk Owner is the owner of this policy and will monitor compliance in the Information Governance Lead Board through audits and ad hoc compliance checks. The SIRO for the Trust is the Director of Strategy and Partnerships |
| **Information Governance Leads Board** | The Information Governance Leads Board is responsible for ensuring that all IG systems, processes and policies are reviewed, developed and monitored in relation to all corporate documentation held within the Trust, whether paper or electronic. |
| **Information Governance Manager** | The Information Governance Manager has a clear responsibility for the management of corporate documentation within the organisation and the post holder reports to the SIRO, who is empowered to make operational decisions and lead on strategic focus.<br><br>The IG Manager's responsibilities include:<br>• Identifying current arrangements for managing corporate documentation, including a survey of existing documentation management systems;<br>• Identifying and understanding all categories of corporate documentation (for example, staff documentation, estates management documents, finance administration papers etc) and their responsible departments or directorates;<br>• Monitoring working practices to verify accuracy, accessibility, integrity and validity of corporate documentation and where there is a lack of compliance, ensure that procedures and general best practice guidelines, reviews and assessments take place to determine how standards should be raised.<br>• Liaising and working with other employees |

| | |
|---|---|
| | responsible for information handling activities, e.g. data protection and the Caldicott function;<br>• Raising awareness of the importance of documentation management throughout the Trust through profile raising and a publicity campaign. |
| **Information Asset Owners (IAOs)** | Information Asset Owners are accountable for the application of this policy to the information assets that they 'own' |
| **All Trust Employees** | • All staff have a personal responsibility for recorded information that they create or that they have some impact upon, whether clinical or corporate, and for adhering to the Trust's suite of Information Governance policy's principles and procedures to help maintain the availability, effectiveness, security and confidentiality of documentation and recorded information.<br>Have a responsibility to:<br>• Support the Trust to achieve its Vision and Values<br>• Follow duties and expectations of staff as detailed in the NHS Constitution – Staff Responsibilities<br>• Every member of staff is responsible for ensuring that they comply with this policy at all times, and for reporting any breaches through the appropriate incident reporting system (ie: Datix). |

## 7. SUBSTANTIVE CONTENT

### 7.1. Documentation & Non Clinical Records Creation

Documentation is created to support the day-to-day running of the Trust's business. A record is created when it meets the legal requirement defined above.

All procedural documents should follow the NGH Policy on Procedural Documents (NGH-PO-001)

Documentation created by the Trust should be arranged in a record-keeping system that will enable the organisation to obtain the maximum benefit from the quick and easy retrieval of information.

Employees should consider the following when creating information:

- what they are recording and how it should be recorded
- why they are recording it
- how to validate information to ensure they are recording the correct data
- how to identify and correct errors and how to report errors if they find them
- the use of information - staff should understand what the records are used for (and therefore why
- timeliness, accuracy and completeness of recording is so important)
- how to update information and how to add in information from other sources

### 7.2. Shared drives

It is important to consider the content of the document when using this option. Where access to the document is to be limited, the creator of the document must ensure that the record is located in a restricted area on the shared drive.

To set up a shared drive a request should be sent to the IT Service Desk giving the:

- Name of drive
- Names of those who would require access
- Parts which need to have access limited

Corporate documentation must never be kept on local drives of personal computers

### 7.3. Filing structures

Filing structures must be easily and quickly understood, enabling quick and efficient filing and retrieval of documentation, where and when required. Structures must also ensure easy identification of applicable retention schedules for these documents and enable implementation of the record disposal recommendations (see appendix 1).

Requests for the creation of electronic departmental folders and for security permissions to be set up or modify shared areas must be made to the IT Service Desk. Requests must come from a senior manager within the directorate or department and include the information in shared folders

### 7.4. Storage of documentation

Where documents exist in paper and electronic format, the filing and naming conventions must mirror each other. The procedures that follow will therefore refer to both paper and electronic records.

### 7.5. Storing paper documents

Equipment used to store current documents on all types of media must provide storage that is safe and secure from unauthorised access, and meet health and safety and fire regulations, but which also allow maximum accessibility of the information commensurate with its frequency of use.

Storage accommodation for current documents must be clean and tidy in order to prevent damage to documents and provide a safe working environment for staff. The following factors should be taken into account:

- Compliance with Health & Safety regulations
- Type(s) of documents to be stored
- Their size and quantities
- Usage and frequency of retrievals
- Security (especially for confidential material)
- The user's needs

Where paper documents are no longer needed to accomplish a business, their placement in a designated secondary storage area may be a more cost-effective and efficient way to store them. Procedures for handling documentation should take full account of the need to preserve important information and keep it confidential and secure.

### 7.6. Non-paper documentation

Digital documentation on various formats must be backed-up/replicated for the purpose of efficient migration to new platforms, and should be designed and scheduled to ensure continuing access to readable information.

The Trust may have collections of visual images – either as artistic images and still photographs (which may be prints, negatives, slides, transparencies, and electronic-readable images) or as moving images (film or video). In the case of photographs, the quality of image available from negatives or original prints should be considered and new prints may be made in cases where the original is deteriorating.

Photograph and film collections assembled by staff through their work within the Trust should be regarded as Public Documentation and subject to the laws and codes of practice detailed in this policy.

Film should be stored in dust-free metal cans and placed horizontally on metal shelves. Microform, sound recordings and videotape should be stored in metal, cardboard or inert plastic containers, and placed vertically on metal shelving.

### 7.7. Scanning

For the purpose of business efficiency and adapting to paperless innovation, the Trust will consider the option of scanning paper documentation into electronic format; this will facilitate issues with storage space. Where this is proposed, the following factors will be taken into consideration:

- The costs of the initial and then any later media conversion to the required standard, bearing in mind the length of the retention period for which the documentation are required to be kept;
- The need to consult in advance with the local Place of Deposit or The National Archives with regard to documentation which may have archival value, as the value may include the format in which it was created; and
- The need to protect the evidential value of the record by copying and storing the record in accordance with British Standards, in particular the „Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically“ (BIP 0008)

The Trust will consider the disposal of paper documentation that have been copied into electronic format and stored in accordance with appropriate standards.

### 7.8. Archiving

Once a record has ceased to be accessed regularly, for example if the member of staff has left the organisation or the record refers to a historic business activity, it is necessary for the practical operation of the organisation that the record be archived to an alternative storage location.

### 7.9. Retention

The minimum length of time that a record is retained by the Trust depends on the type of record. In most areas, The Trust has adopted the minimum retention schedules published in the Records Management: NHS Code of Practice (2009): D1 and D2 respectively. (Please see appendix A for Corporate Records Retention Schedules).

Documentation, in whatever format they are held, may be retained for longer than the minimum retention periods, but should not normally be kept for more than 20 years with the exception of a few records e.g. COSHH.

Requests for extended preservation are subject to approval by the Information Governance Leads Board. This may only happen on grounds of historical archival value, relevance to research or other preserved documentation.

Information Asset Owners are responsible for determining if a record for which they are accountable should be retained for longer than the minimum retention period. This should be listed in a local retention schedule and communicated to all Information Asset Administrators.

### 7.10. Movement and Tracking of Documentation

The physical movement of documentation should be undertaken in a safe and secure way and should always be tracked, i.e. the person sending the information should inform the person transporting the information and the intended recipient what information has been sent, and the recipient should confirm on receipt that the information has been received, unless a system is in use to allow this to be done automatically.

Documentation transported between sites/departments MUST be enclosed in, sealed pouches or bags, securely enclosed trolleys or other appropriate sealed, sealed and locked or tamper evident container, and appropriately labelled i.e. confidential, and clearly addressed to the recipient.

For higher risk documents transfers e.g. child protection, they must also be marked as “to be opened by addressee only”. A separate risk assessment is required for such documentation and should be subject to a local procedure operated by the Information Asset Administrator and approved by the Information Asset Owner.

Only Trust’s approved transport services may be used, as these should be appropriate for the level of risk associated with the content and quantity of documentation. Documentation should be transported between sites/departments by authorised staff, including:

- Internal transport systems
- Authorised courier service
- Off-site documentation storage supplier

Tracking mechanisms must record the following (minimum) information:

- The item reference number or other identifier
- A description of the item (e.g. the file title)
- The person, unit or department, or place to which it is being sent
- The date of the transfer to them

Tracking systems will be reviewed and implemented in liaison with the Trust’s Information Governance Manager. Common methods for manually tracking the movements of active documentation include:

- A paper register – a book, diary, or index card to record transfers
- File “on loan” (library-type) cards for each absent file, held in alphanumeric order
- File “absence” or “tracer” cards put in place of absent files

Documentation in transit must never be left unattended. Staff must obtain approval of the responsible Information Asset Administrator each time they remove any record from Trust’s premises. If more than 10 documents are to be removed from site, the permission of an accountable manager/asset owner must be obtained. Return of documentation taken by individuals must also be formally witnessed and noted.

Electronic documentation containing confidential or Personal Identifiable Data (PI.D) must only be sent out via, and to an NHS.net account; this ensures they are encrypted. Staff can contact the IT Help desk for NHS.net account set up.

For guidance on the use of fax, email and postal transfer of documentation please refer to the following:

- NGH Transmission of Confidential Information (Safe Haven) Policy
- NGH Data Protection and Confidentiality Policy
- Confidentiality Code of Conduct (imbedded in NGH staff Contracts)

### 7.11. Disposal and Destruction of Documentation

Documentation selected for archival preservation and no longer in regular use should be archived according to the National Archives guidelines.

Destruction of records must be clearly documented. A log of destroyed corporate documentation should be kept and maintained locally for all record destructions. The contracted disposal/destruction company will provide also the Trust with consignment notes for each consignment sent for destruction.

The Trust carries out regular duty of care visits to the contracted company to ensure compliance. Further information is available in the Trust's Waste Management Policy (NGH-PO-650)

### 7.12. Exceptions

Where a document marked for destruction is the subject of a request under the Freedom of Information Act, destruction should be delayed until:

- The disclosure has taken place.
- The complaint and appeal provisions have been exhausted if the decision not to release the information was taken.

Hardcopy documentation to be preserved must be clearly marked on the cover stating the record should not be destroyed together with the date, name and signature of the Information Asset Administrator.

### 7.13. Right of Access

The right of access to records, particularly health records is a complex area of law. Guidance is published by the Department of Health, Guidance to Access to Health Records Requests (Gateway reference 13214).

Staff responsible for Patient Advisory Liaison and Clinical Assessment would have access to health records, and may be asked to provide access to these records. These staff should refer requests to the correct person in the Trust (Health Records Manager) before allowing access to records, either directly or by sharing the information the record contains by other means.

### 7.14. Freedom of Information (FOI)

It is particularly important under FOI legislation that the disposal of records, which is defined at the point in their lifecycle when they are either transferred to an archive or destroyed, is undertaken in accordance with clearly established policies.

Records that are subject to Freedom of Information Act (FOIA) i.e. does not contain Person Identifiable Information will be listed as information assets in the Information Asset Register (e.g. applicable finance systems). Request for disclosure of information from Information Assets Register under the FOIA will be managed by the Information Governance Team and should be forwarded to them immediately on receipt.

## 8. IMPLEMENTATION & TRAINING

A number of bodies monitor NHS performance in respect of Records Management. The Healthcare Commission will be monitoring a core governance standard relating to broad records management as part of its annual assessment of performance.

The Audit Commission regularly conducts studies into records management and related information quality issues. The Department of Health collects performance details as part of the annual information governance toolkit assessment and these will inform the work of both the Healthcare Standards Commission and the Audit Commission.

To ensure that staff have acquired the knowledge necessary for compliance with this policy, relevant staff will be assessed as a part of the implementation of their mandatory IG Training.

## 9. MONITORING & REVIEW

| Minimum policy requirement to be monitored | Process for monitoring | Responsible individual/ group/ committee | Frequency of monitoring | Responsible individual/ group/ committee for review of results | Responsible individual/ group/ committee for development of action plan | Responsible individual/ group/ committee for monitoring of action plan |
|---|---|---|---|---|---|---|
| Minimum compliance with this policy will be measured against applicable requirements in the IG Toolkit, | The Trust will use a variety of methods to monitor compliance with the processes in this document, including as a minimum the following two methods:<br>Standards Compliance<br>Levels of compliance with this policy will be measured against applicable requirements in the IG Toolkit, CQC Standards for Better Health and NHSLA requirements. | Information Governance Manager | Annually | Information Governance Leads Board | Information Governance Leads Board. | Information Governance Leads Board. |

## 10. REFERENCES & ASSOCIATED DOCUMENTATION

British Standards Institution (2008) BIP 0008-1:2008: *Evidential weight and legal admissibility of information stored electronically: Code of Practice for the implementation of BS 10008*. Milton Keynes: BSI

Care Quality Commission (2015) *National Standards*. [online]. Available from: http://www.cqc.org.uk/content/national-standards [Accessed 17th February 2014]

*Charities Act 1993*. (c.10). London: HMSO

Data Protection Act 1998 (c.29) [online] London, HMSO. Available from: http://www.legislation.gov.uk/ukpga/1998/29 [Accessed 15 January 2014]

Department of Health (2013). *NHS Constitution: the NHS belongs to us all.* [online]. London. Department of Health. Available from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/170656/NHS_Constitution.pdf [Accessed 1 June 2013]

Department of Health (2010) *Guidance for Access to Health Records Requests*. [online]. London: DH. Available from: http://webarchive.nationalarchives.gov.uk/20130107105354/http://www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/@dh/@en/@ps/documents/digitalasset/dh_113206.pdf [Accessed 17th February 2014]

Department of Health (2009) *Records Management: NHS Code of Practice: Part 2*. 2nd ed. [online]. London: DH. Available from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200139/Records_Management_-_NHS_Code_of_Practice_Part_2_second_edition.pdf [Accessed 15 January 2014]

Department of Health (2006) *Records Management: NHS Code of Practice: Part 1*. [online]. London: DH. Available from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200138/Records_Management_-_NHS_Code_of_Practice_Part_1.pdf [Accessed 17th February 2014]

Department of Health (2003) *Confidentiality: NHS Code of Practice*. [online]. London: DH. Available from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200146/Confidentiality_-_NHS_Code_of_Practice.pdf [Accessed 17th February 2014]

Department of Health (n.d) *Information Governance Toolkit: Homepage*. [online]. Available from: https://nww.igt.hscic.gov.uk/ [Accessed 17th February 2014]

Department of Health, Social Services and Public Safety (2013) *The Common Law Duty of Confidentiality*. [online]. Available from: http://www.dhsspsni.gov.uk/gmgr-annexe-c8 [Accessed 17th February 2014].

Cabinet Office, Government Security Classifications (2014) [online]. Available from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251480/Government-Security-Classifications-April-2014.pdf .[Accessed 20th January 2015].

*Environmental Information Regulations 2005.* SI2004/3391. London: HMSO

*Freedom of Information Act 2000* (c.36) [online] London. HMSO. Available from: http://www.legislation.gov.uk/ukpga/2000/36/contents [Accessed 15 January 2014]

National Information Governance Board for Health and Social Care (NIGB) (2011) *The Care Record Guarantee Our Guarantee for NHS Care Records in England*. London: NIGB

NHS Litigation Authority (2012) *The NHS Litigation Authority: Homepage*. [online]. Available from: http://www.nhsla.com/ [Accessed 17th February 2014]

Northampton General Hospital NHS Trust (2014) *Procedural Documents.* NGH-PO-001. Northampton: NGHT

Northampton General Hospital NHS Trust (2014) *Waste Management.* NGH-PO-650. Northampton: NGHT

Northampton General Hospital NHS Trust (2013) *Equality and Human Rights Strategy 2013-2016*. Northampton: NGHT

Northampton General Hospital NHS Trust (2012) *Transmission of Confidential Information (Safe Haven)*. NGH-PO-066. Northampton: NGHT

*Public Records Act 1958*. (c. 51, 6 and 7 Eliz 2). [online] London: HMSO. Available from: http://www.legislation.gov.uk/ukpga/Eliz2/6-7/51 [Accessed 25 March 2014]

Secretary of State for Constitutional Affairs (2004) *Secretary of State for Constitutional Affairs' Code of Practice on the discharge of public authorities' functions under Part 1 of the Freedom of Information Act 2000, Issued under section 45 of the Act. HC 33*. [online]. London: Stationery Office. Available from: http://www.official-documents.gov.uk/document/hc0405/hc00/0033/0033.pdf [Accessed 17th February 2014]

Surrey Health Informatics Services and Sussex Health Informatics Services (2007) *NHS Records Retention Schedules: A guide to Records Management: Records Management explained*. [online]. Surrey Health Informatics Service and Sussex Health Information Services. Available from https://www.igt.hscic.gov.uk/KnowledgeBaseNew/Surrey%20HIS_Records%20Management%20Explained%20-%20Retention%20Schedules.pdf [Accessed 15 January 2014]

The National Archives (n.d) *Records Management Guidance*. [online]. Available from: http://www.nationalarchives.gov.uk/information-management/projects-and-work/records-management-guidance.htm [Accessed 17th February 2014]

## APPENDICES

### Appendix 1: RETENTION & DISPOSAL SCHEDULE

**This document is taken from Annex D2 of the NHS Code of Practice. It must be noted that some of the records listed may not be representative of the records held by NGH departments.**

### Corporate (Non Health) Records Retention Schedule

The National Archives (see note 1 below) should be consulted where a longer retention period than 30 years is required, or for any pre-1948 records. The following types of record are covered by this retention schedule (regardless of the media on which they are held, including paper, electronic, images and sound):

- Administrative records (including personnel, estates, financial and accounting records, and notes associated with complaint handling)
- Photographs, slides and other images (non-clinical)
- Microform (i.e. microfiche / microfilm)
- Audio and video tapes, cassettes, CD-ROM's etc
- E-mails
- Computerised records; and
- Scanned documents

The retention schedule is split into the following types of records:

- Corporate & Organisational
- Finance
- Estates, Supplies & Purchasing
- Human Resources
- IM&T

### Notes

**Note 1 – An organisation with an existing relationship with an approved Place of Deposit should consult the Place of Deposit in the first instance. Where there is no pre-existing relationship with a Place of Deposit, organisations should consult the National Archives.**

The criteria below are designed to give guidance on how long records should be kept for business purposes and the identification of records of permanent value.

Records no longer required for business use should be reviewed under the following criteria so that ill-considered destruction is avoided. This schedule identifies minimum retention periods.

Whenever the schedule is used, the guidelines below should be followed:

- ✓ Local business requirements/instructions must be considered before activating retention periods in this schedule.
- ✓ Decisions should also be considered in the light of the need to preserve records whose use cannot be anticipated fully at the present time, but which may be of value to future generations.
- ✓ Recommended minimum retention periods should start from the end of the calendar or accounting year following the last entry on the document.
- ✓ The provision of the Data Protection Act 1998 must be complied with.

The schedule does not seek to cater for all eventualities: managers need to consider whether exceptional circumstances e.g. the events of local or national significance reflected in the records, require the long-term preservation of the records.

**Corporate & Organisational**

| Record Type | Minimum Retention Period (Years) | Destruction |
|---|---|---|
| Accident Form | 10 Years | Destroy under confidential conditions |
| Accident Register | 10 Years | Destroy under confidential conditions |
| Advance Letters | 6 Years | Destroy |
| Agendas of Board Meetings, Committees, Sub-Committees | 30 Years | See Note 1 |
| Agendas (other) | 2 Years | Destroy under confidential conditions |
| Annual/Corporate Records | 3 Years | Destroy under confidential conditions |
| Assembly/Parliamentary Questions, MP Enquiries | 10 Years | Destroy under confidential conditions |
| Audit Records (internal & external) | 2 Years from completion of audit | Destroy under confidential conditions |
| Business Plans (incl. local delivery plans) | 20 Years | Destroy |
| CCTV Images | 31 Days | Destroy under confidential conditions |
| *Commissioning Decisions*<br>- Appeal Documentation<br>- Decisions Documentation | 6 Years from appeal decision date<br>6 Years from decision date | Destroy under confidential conditions<br>Destroy under confidential conditions |

| | | |
|---|---|---|
| *Complaints*<br><br>- Correspondence, Investigation & Outcomes<br><br>- Returns made to DoH | 8 Years from action completion<br><br>Files closed annually, kept for 6 years | Destroy under confidential conditions<br><br>Destroy under confidential conditions |
| Data Input Forms | 2 Years | Destroy under confidential conditions |
| Chaplaincy records | 2 years | May have archival value – see note 1 |
| Diaries (office) | 1 Year after end of Calendar year | Destroy under confidential conditions |
| Family Health Service Appeals Authority tribunal and case files | Case files – 10 yearsDecision records – until individual's 80th birthday | |
| *'Find-a-doc' Records*<br><br>- Contact Sheets & Letters<br><br>- Assignment Cases/Letters<br><br>- Records of negotiations with GMS Contract Managers re. Patient registration with GP | <br><br><br>6 Months<br><br>2 Years<br><br>2 Years | <br><br><br>Destroy under confidential conditions<br><br>Destroy under confidential conditions<br><br>Destroy under confidential conditions |
| Freedom of Information Requests | 3 Years after full disclosure<br><br>10 Years if information redacted/not disclosed | Destroy under confidential conditions |

| | | |
|---|---|---|
| Health & Safety Documentation | 3 Years | Destroy under confidential conditions |
| History of Organisation or Predecessors, its Organisation & Procedures (eg. Establishment order) | 30 Years | See Note 1 |
| Indices (Records Management) | Registry lists of public records marked for permanent preservation, or containing the record of management of public records – 30 Years.<br><br>File lists and document lists where public records or their management are not covered – 30 Years | See Note 1 / Destroy under confidential conditions |
| Litigation Dossiers (complaints including accident/incident reports) | 10 Years | Destroy under confidential conditions |
| Manuals – Policy & Procedure (administrative and clerical, strategy documents) | 10 Years after system life | See Note 1 |
| Meetings & Minute Papers of major committees and sub-committees (master copies) | 30 Years | See Note 1 |
| Meetings & Minute Papers (other, including reference copies of major committees) | 2 Years | Destroy under confidential conditions |

| | | |
|---|---|---|
| Mental Health Act administration records | 5 Years | Destroy under confidential conditions |
| Mortgage Documents (acquisition, transfer and disposal) | 6 Years after repayment | See Note 1 |
| Nominal Rolls | 6 (maximum) | Destroy under confidential conditions/See Note 1 |
| *Papers of Minor of Short-lived importance not covered elsewhere*<br><br>- Advertising Matter<br><br>- Covering Letters<br><br>- Reminders<br><br>- Letters making appointments<br><br>- Anonymous or unintelligible letters<br><br>- Drafts<br><br>- Duplicates of documents known to be preserved elsewhere (unless they have important minutes on them)<br><br>- Indices and registers compiled for temporary purposes<br><br>- Routine reports<br><br>- Punched cards | 2 Years after matter of settlement to which they relate | Destroy under confidential conditions/see Note 1 |

| | | |
|---|---|---|
| - Other documents that have ceased to be of value on settlement of the matter involved | | |
| Patient Advice & Liaison Service (PALS) records | 10 Years after case closure | Destroy under confidential conditions |
| Patient information leaflets | 6 Year after leaflet has been superseded | See Note 1 |
| Patient Surveys (re. access to surveys etc) | 2 Years | Destroy under confidential conditions |
| Press Cuttings | 1 Year after end of Calendar year | Destroy |
| Press Releases | 7 Years | See Note 1 |
| Project Files (over £100,000) on termination, including abandoned or deferred projects | 6 Years | See Note 1 |
| Project Files (less than £100,000) on termination | 2 Years | Destroy under confidential conditions |
| Project Team Files | 3 Years | Destroy under confidential conditions |
| Public Consultations e.g. about future provision of services | 5 Years | Destroy under confidential conditions |

| | | |
|---|---|---|
| Quality Assurance Records (eg. Healthcare Commission, Audit Commission, King's Fund Organisational Audit, Investors in People) | 12 Years | Destroy under confidential conditions |
| Receipts for registered and recorded mail | 2 Years following the end of the financial year to which they relate | Destroy under confidential conditions |
| Records documenting the archiving, transfer to public records archive or destruction of records | 30 Years | See Note 1 |
| Reports (major) | 30 Years | See Note 1 |
| Requests to access to records, other than Freedom of Information or subject access requests | 6 Years after last action | Destroy under confidential conditions |
| Requisitions | 18 Months | Destroy under confidential conditions |
| Serious Incident Files | 30 Years | See Note 1 |
| Specifications (e.g. Equipment, services) | 6 Years | Destroy under confidential conditions |

**Finance**

| Record Type | Minimum Retention Period (Years) | Destruction |
|---|---|---|
| Accounts – annual (final – one set only) | 30 Years | See Note 1 |
| Accounts – minor records (pass books, paying-in slips, cheque counterfoils, cancelled/discharged cheques (for cheques bearing printed receipts, see Receipts), accounts of petty cash expenditure, travel and subsistence accounts, minor vouchers, duplicate receipt[t books, income records, laundry lists and receipts) | 2 Years from audit completion | Destroy under confidential conditions |
| Accounts – working papers | 3 Years from audit completion | Destroy under confidential conditions |
| Advice notes (payment) | 1.5 Years | Destroy under confidential conditions |
| Audit records (internal & external audit) – original documents | 2 Years from audit completion | Destroy under confidential conditions |
| Audit reports – internal & external (including management letters, value for money reports and system/final accounts memoranda) | 2 Years after form completion by statutory auditor | Destroy under confidential conditions |
| Bank statements | 2 Years from audit completion | Destroy under confidential conditions |

| | | |
|---|---|---|
| Banks Automated Clearing System (BACS) records | 6 Years after year end | Destroy under confidential conditions |
| Benefactions (records of) | 5 Years after end of financial year in which the trust monies become finally spent or the gift in kind is accepted. In cases where the Benefaction Endowment Trust fund/capital/interest remains permanent, records should be permanently retained by the organisation | See Note 1 |
| Bills, receipts & clearing cheques | 6 Years | Destroy under confidential conditions |
| Budgets (including working papers, reports, virements and journals) | 2 Years from audit completion | Destroy under confidential conditions |
| Capital charges data | 2 Years from audit completion | Destroy under confidential conditions |
| Capital paid invoices (see Invoices) | | |
| Cash books | 6 Years after the end of the financial year to which they relate | Destroy under confidential conditions |
| Cash sheets | 6 Years after the end of the financial year to which they relate | |

| | | |
|---|---|---|
| Contracts - financial | Approval files – 15<br><br>Approved suppliers list – 11 | Destroy under confidential conditions |
| Contracts – non-sealed (property) on termination | 6 Years after contract termination | Destroy under confidential conditions |
| Contracts – non-sealed (other) on termination | 6 Years after contract termination | Destroy under confidential conditions |
| Contracts – sealed (and associated records) | 15 (minimum), after which they should be reviewed | See Note 1 |
| Contractual agreements with hospitals or other bodies outside the NHS, including papers relating to financial settlements made under the contract (e.g. Waiting list initiative, private finance initiative) | 6 Years after the end of the financial year to which they relate | Destroy under confidential conditions |
| Cost accounts | 3 Years after the end of the financial year to which they relate | Destroy under confidential conditions |
| Creditor payments | 3 Years after the end of the financial year to which they relate | Destroy under confidential conditions |
| Debtor's records – cleared | 2 Years from audit completion | Destroy under confidential conditions |
| Debtor's records - uncleared | 6 Years from audit completion | Destroy under confidential conditions |

| | | |
|---|---|---|
| Demand notes | 6 Years after the end of the financial year to which they relate | Destroy under confidential conditions |
| Estimates, including supporting calculations and statistics | 3 Years after the end of the financial year to which they relate | Destroy under confidential conditions |
| Excess fares | 2 Years after the end of the financial year to which they relate | Destroy under confidential conditions |
| Expense claims, including travel and subsistence claims, and claims and authorisations | 5 Years after the end of the financial year to which they relate | Destroy under confidential conditions |
| Fraud case files/investigations | 6 Years | Destroy under confidential conditions |
| Fraud national proactive exercises | 3 Years | Destroy under confidential conditions |
| Funding data | 6 Years after the end of the financial year to which they relate | Destroy under confidential conditions |
| General Medical Services payments | 6 Years after year end | Destroy under confidential conditions |
| Invoices | 6 Years after the end of the financial year to which they relate | Destroy under confidential conditions |

| | | |
|---|---|---|
| Ledgers, including cash books, ledgers, income and expenditure journals, nominal rolls, non-exchequer funds records (patient monies) | 6 Years after the end of the financial year to which they relate | Destroy under confidential conditions |
| Non-exchequer funds records (i.e. funding received by the organisation that does not directly relate to patient care e.g. charitable funds) | 30. Company charities are required by company law to keep their accounts and accounting records for at least three years but the Charity Commission recommends they be kept for at least 6 Years. The majority of non-company charities must keep their accounts and accounting records for six years (Part VI Charities Act 1993) | Although technically exempt from the Public Records Act, it would be appropriate for authorities to treat these records as if they were not exempt |
| Patient Monies (i.e. smaller sums of donated money) | 6 Years | Destroy under confidential conditions |
| PAYE Records | 6 Years after termination of employment | Destroy under confidential conditions |
| Payments | 6 Years after year end | Destroy under confidential conditions |
| Payroll (i.e. list of staff in the pay of the organisation) | 6 Years after termination of employment | Destroy under confidential conditions for superannuation purposes, organisations may wish to retain such records until the subject reaches benefit age |

| | | |
|---|---|---|
| Positive predictive value performance indicators | 3 Years | Destroy under confidential conditions |
| Private Finance Initiative (PFI) | 30 Years | See Note 1 |
| Receipts | 6 Years after the end of the financial year to which they relate | Destroy under confidential conditions |
| Salaries (see Wages) | | |
| Superannuation accounts | 10 Years | Destroy under confidential conditions |
| Superannuation registers | 10 Years | Destroy under confidential conditions |
| Tax forms | 6 Years | Destroy under confidential conditions |
| Trust documents without permanent relevance/not otherwise mentioned | 6 Years | Destroy under confidential conditions |
| Trusts administered by Strategic Health Authorities (terms of) | 30 Years | See Note 1 |
| VAT records | 6 Years after the end of the financial year to which they relate | Destroy under confidential conditions |
| Wages/salary records | 10 Years after termination of employment | Destroy under confidential conditions. For superannuation purposes, organisations may wish to retain such records until the subject reaches benefit age |

**Estates, Supplies & Purchasing**

| Record Type | Minimum Retention Period (Years) | Destruction |
|---|---|---|
| Approval files (contracts) | 6 Years after the end of the year the contract expired | Destroy under confidential conditions |
| Approved suppliers lists | 11 Years | Destroy under confidential conditions |
| Buildings and engineering works, including major projects abandoned or deferred – key records (e.g. final accounts, surveys, site plans, bills of quantities) | 30 Years | See Note 1 |
| Buildings and engineering works, including major projects abandoned or deferred – town and country planning matters and all formal contract documents (e.g. executed agreements, conditions of contract, specifications, 'as built' record drawings, documents on the appointment and conditions of engagement of private buildings and engineering consultants) | 30 Years | See Note 1 |
| Buildings – papers relating to occupation of the building (but not health and safety information) | 3 Years after occupation ceases | Destroy under confidential conditions |

| | | |
|---|---|---|
| Deeds of Title | Retain while the organisation has ownership of the building unless a Land Registry certificate has been issued, in which case the deeds should be placed in an archive. If there is no Land Registry certificate, the deeds should pass on with the sale of the building | See Note 1 |
| Delivery notes | 2 Years after the end of the financial year to which they relate | Destroy under confidential conditions |
| Drawings – plans and buildings (architect signed, not copies) | Lifetime of the building to which they relate | See Note 1 |
| Engineering works – plans and building records | Lifetime of the building to which they relate | See Note 1 |
| Equipment – records of non-fixed equipment, including specification, test records, maintenance records and logs | 11 Years.<br><br>If the records relate to vehicles (ambulances, responder cars, fleet vehicles etc) and where the vehicle no longer exists, providing there is a record that it was scrapped, the records can be destroyed | Destroy under confidential conditions |
| Inspection reports (e.g. boilers, lifts) | Lifetime of installation. If there is any measurable risk of a liability in respect of installations beyond their operational lives, the records should be retained indefinitely | See Note 1 |

| | | |
|---|---|---|
| Inventories of furniture, medical and surgical equipment not held on store charge and with a minimum life of 5 years | Keep until next inventory | See Note 1 |
| Inventories of plant and permanent or fixed equipment | 5 Years after date of inventory | See Note 1 |
| Land surveys/registers | 30 Years | See Note 1 |
| Leases – the grant of leases, licences and other rights over property | Period of the lease plus 12 Years | Destroy under confidential conditions |
| Maintenance contracts (routine) | 6 Years from end of contract | Destroy under confidential conditions |
| Manuals (operating) | Lifetime of equipment | Review if issues (e.g. HSE) are outstanding |
| Medical device alerts | Retain until updated or withdrawn (check MHRA website) | Destroy under confidential conditions |
| Photographs of buildings | 30 Years | See Note 1 |
| Plans – buildings (as built) | Lifetime of building | May have historical value – See Note 1 |
| Plans – buildings (detailed) | Lifetime of building | May have historical value – See Note 1 |
| Plans – engineering | Lifetime of building | See Note 1 |
| Products (liability) | 11 Years | Destroy under confidential conditions |
| Property acquisition dossiers | 30 Years | See Note 1 |
| Property disposal dossiers | 30 Years | See Note 1 |

| | | |
|---|---|---|
| Radioactive waste | 30 Years | See Note 1 |
| Site files | Lifetime of site | See Note 1 |
| Stock control reports | 18 Months | Destroy under confidential conditions |
| Stores records – major (e.g. stores ledgers) | 6 Years | Destroy under confidential conditions |
| Stores records – minor (e.g. requisitions, issue notes, transfer vouchers, goods received books) | 18 Months | Destroy under confidential conditions |
| Structure plans (organisational charts) i.e. the structure of the building plans | Lifetime of building | See Note 1 |
| Supplies records – minor (e.g. invitations to tender and inadmissible tenders, routine papers relating to catering and demands for furniture, equipment, stationery and other supplies) | 18 Months | Destroy under confidential conditions |
| Surveys – building and engineering works | Lifetime of building or installation | See Note 1 |
| Tenders (successful) | Tender period plus 6 Year limitation period | Destroy under confidential conditions |
| Tenders (unsuccessful) | 6 Years | Destroy under confidential conditions |

**Human Resources**

| Record Type | Minimum Retention Period (Years) | Destruction |
|---|---|---|
| Consultants (records relating to the recruitment of) | 5 Years | Destroy under confidential conditions |
| CVs for non-executive directors (successful applicants) | 5 Years following term of office | Destroy under confidential conditions |
| CVs for non-executive directors (unsuccessful applicants) | 2 Years | Destroy under confidential conditions |
| Duty rosters i.e. organisation for department rosters, not the ones held on the individual's record | 4 Years after the year to which they relate | Destroy under confidential conditions |
| Industrial relations (not routine staff matters), including industrial tribunals | 10 Years | Destroy under confidential conditions |
| Job advertisements | 1Year | Destroy |
| Job applications (successful) | 3 Years following termination of employment | Destroy under confidential conditions |
| Job applications (unsuccessful) | 1 Year | Destroy under confidential conditions |
| Job descriptions | 3 Years | Destroy under confidential conditions |

| | | |
|---|---|---|
| Leavers' dossiers | 6 Years after the individual has left. Summary to be retained until individual's 70th birthday or until 6 years after cessation of employment if aged over 70 years at the time.<br><br>The summary should contain everything except attendance books, annual leave records, duty rosters, clock cards, timesheets, study leave applications, training plans | Destroy under confidential conditions/See Note 1 |
| Letters of appointment | 6 Years after employment has terminated or until 70th birthday, whichever is later | Destroy under confidential conditions |
| Nurse training records (from hospital-based nurse training schools prior to the introduction of academic-based training) | 30 Years | See Note 1 |
| PAYE Records | 6 Years after termination of employment | Destroy under confidential conditions |
| Payroll (i.e. list of staff in the pay of the organisation) | 6 Years after termination of employment | Destroy under confidential conditions for superannuation purposes, organisations may wish to retain such records until the subject reaches benefit age |
| Pension forms (all) | 7 Years | Destroy under confidential conditions |

| | | |
|---|---|---|
| Personnel/human resource records – major (e.g. personal files, letters of appointment, contracts, references and related correspondence, registration authority forms, training records, equal opportunity monitoring forms (if retained))<br><br>NB: includes locum doctors | 6 Years after the individual leaves service, at which time a summary of the file must be kept until the individual's 70th birthday. Summary to be retained until individual's 70th birthday or until 6 years after cessation of employment if aged over 70 years at the time.<br><br>The summary should contain everything except attendance books, annual leave records, duty rosters, clock cards, timesheets, study leave applications, training plans | See Note 1 |
| Personnel/human resource records – Appraisal documents | 6 Years after the year to which it relates | Destroy under confidential conditions |
| Personnel/human resource records – minor (e.g. attendance books, annual leave records, duty rosters (i.e. duty rosters held on the individual's record not the organisation or departmental rosters), clock cards, timesheets (relating to individual staff members))<br><br>NB: includes locum doctors | 2 Years after the year to which they relate | Destroy under confidential conditions |

| | | |
|---|---|---|
| Salaries (see Wages) | | |
| Staff car parking permits | 3 Years | Destroy under confidential conditions |
| Study leave applications | 5 Years | Destroy under confidential conditions |
| Timesheets (for individual members of staff) | 2 Years after the year to which they relate.<br><br>NB: timesheets (for all individuals including locum doctors) held on the personnel record are minor records – retain for 2 Years.<br><br>Timesheets held elsewhere – i.e. on the ward retain for 6 months (as the master timesheet is held on the personnel file) | Destroy under confidential conditions |
| Training plans | 2 Years | Destroy under confidential conditions |
| Wages/salary records | 10 Years after termination of employment | Destroy under confidential conditions. For superannuation purposes, organisations may wish to retain such records until the subject reaches benefit age |

**IM & T**

| Record Type | Minimum Retention Period (Years) | Destruction |
|---|---|---|
| Documentation relating to computer programmes written in-house | Lifetime of software | Destroy under confidential conditions |
| Software licenses | Lifetime of software | Destroy under confidential conditions |

**Research and Development Records**

| Clinical Trials of Investigational Medicinal Products (CTIMPs) | | |
|---|---|---|
| **Record Type** | **Minimum Retention Period (Years)** | **Destruction** |
| Trial Master File (responsibility of Sponsor & Chief Investigator to ensure that documents are retained) | Five years after the conclusion of the trial | Destroy under confidential conditions |
| Trial Subject's Medical Files (Sponsor & Chief Investigator's responsibility to ensure retained) | Five years after the conclusion of the trial.<br><br>There should be a flag or divider in health records for documents pertaining to research indicating that the patient has been recruited to a clinical trial or other research | Destroy under confidential conditions |
| Marketing authorisation (holders must arrange for essential clinical trial documents (including case report forms) other than subject's medical files, to be kept by the owners of the data): | 15 years after completion or discontinuation of the trial,<br>or<br>Two years after the granting of the last marketing authorisation in the European Community and when there are no pending | Destroy under confidential conditions |

| | | |
|---|---|---|
| | or contemplated marketing applications in the European Community,<br>or<br>Two years after formal discontinuation of clinical development of the investigational product. | |
| Trial subject's medical files | Retain in accordance with applicable legislation and in accordance with the maximum period of time permitted by the hospital, institution or private practice NB Documents can be retained for a longer period, however, if required by the applicable regulatory requirements or by agreement with the sponsor. It is the responsibility of the sponsor to inform the hospital, institution or practice as to when these documents no longer need to be retained. | Destroy under confidential conditions |
| All other documentation pertaining to the trial (retention of documentation is the responsibility of the sponsor or other owner of the data) | Retain as long as the product is authorised. | Destroy under confidential conditions |
| Final Report (responsibility of sponsor or subsequent owner's to retain documents) | Five years after the medicinal product is no longer authorised. | Destroy under confidential conditions |
| **Data Collected in the Course of Research** | | |
| Data collected in the course of research | Retain for an appropriate period, to allow further analysis by the original or other research teams subject to consent, and to support monitoring by regulatory and other authorities. | Destroy under confidential conditions |

## Appendix 2: PROTECTIVE MARKING SCHEME

### Classification of NHS Information - Marking Guidance for NGH Staff

All information the Trust collects, stores, processes, generates or shares to deliver services and conduct business has intrinsic value and requires an appropriate degree of protection. Every member of staff has a responsibility to handle the information or data that they access appropriately, irrespective of whether it is confidential or not

New Government Security Classifications (published April 2014) have been implemented to assist you in deciding how to share and protect information. Three simplified levels of security classifications for information assets are now in effect. The new levels are;

**OFFICIAL**
Definition – ALL routine public sector business, operations and services should be treated as OFFICIAL. The Trust will operate exclusively at this level including when necessary the subset categories of OFFICIAL-SENSITIVE: COMMERCIAL and OFFICIAL–SENSITIVE: PERSONAL where applicable. See Table 1 for examples.

**SECRET**
Definition – Very sensitive government (or partners) information that requires protection against the highly capable threats, such as well-resourced and determined threat agents and highly serious organised crime groups.

**TOP SECRET**
Definition – Exceptionally sensitive Government (or partners) information assets that directly support (or threaten) the national security of the UK or allies and requires extremely high assurance or protection against highly bespoke and targeted attacks.

The new classification procedure should not be applied retrospectively. All information used by the Trust is by definition 'OFFICIAL.' It is highly unlikely The Trust will work with 'SECRET' or 'TOP SECRET' information.

Things to note about OFFICIAL information:

- Ordinarily OFFICIAL information does not need to be marked as non-confidential information.

- A limited subset of OFFICIAL information could have more damaging consequences if it were accessed by individuals by accident or on purpose, lost, stolen or published in the media. This subset of information should still be managed within the OFFICIAL classification tier, but should have additional measures applied in the form of OFFICIAL-SENSITIVE.
  This marking is necessary for person-identifiable information and commercially sensitive information and is applicable to paper and electronic documents/records.

- In additional to the marking of OFFICIAL-SENSITIVE further detail may be required regarding the content of the document or record, i.e. OFFICIAL – SENSITIVE: COMMERCIAL

**NHS Confidential**

The Trust has adopted the new government classification scheme for corporate information as it is an expectation from the DH for all Arms Length bodies (ALBs) to comply with. Our approach will satisfy any corporate communications with DH, other government departments, NHS Trusts and ALBs.

In the interim, some NHS organisations may still work to existing IG guidance; consequently any information received from an NHS organisation may be marked as NHS Confidential which should then be treated as OFFICIAL – SENSITIVE depending on its type.

**How to handle and store OFFICIAL information;**
All Trust staff have the responsibility to handle OFFICIAL information with care by:

- Applying clear desk policy
- Information sharing with the right people
- Taking extra care when sharing information with external partners i.e. send information to named recipients at known addresses, sending via secure modes of transfer.
- Locking your screen before leaving the computer
- Using discretion when discussing information out of the office

**How to handle and store OFFICIAL – SENSITIVE information;**
All OFFICIAL-SENSITIVE material including documents, media and other material should be physically secured to prevent unauthorised access. As a minimum, when not in use, all OFFICIAL-SENSITIVE: PERSONAL or OFFICIAL-SENSITIVE: COMMERCIAL material should be stored in a secure encrypted device such as a secure drive or encrypted data stick, lockable room, cabinets or drawers.

- Always apply appropriate protection and comply with the handling rules (please refer to the Information Security Policy)
- Always question whether your information may need stronger protection or access restriction.
- Make sure documents are not overlooked when working remotely or in the community, work digitally if possible to minimise the risk of leaving papers on trains, etc.
- Only print sensitive information when absolutely necessary
- Send sensitive information by the secure postal, email route or use encrypted data transfers (please refer to the transfer of Confidential Information Policy – Safe Haven)
- Use only Trust approved portable devices
- Store information securely when not in use and use a locked cabinet/drawer if paper is used
- If faxing the information, make sure the recipient is expecting your fax and double check their fax number (follow faxing good practice guidelines)
- Take extra care to be discreet when discussing sensitive issues by telephone, especially when in public areas and minimise sensitive details.

**Table 1 – Descriptors that may be used with OFFICIAL-SENSITIVE: COMMERCIAL OR OFFICIAL-SENSITIVE: PERSONAL**

| Category | Definition | Marking |
|---|---|---|
| Appointments (Staff) | Concerning actual or potential appointments not yet announced | OFFICIAL-SENSITIVE: COMMERCIAL |
| Barred | Where<br>• there is a statutory (Act of Parliament or European Law) prohibition on disclosure, or<br>• disclosure would constitute a contempt of Court (information the subject of a court order) | OFFICIAL-SENSITIVE: COMMERCIAL |
| Board | Documents for consideration by an organisation's Board of Directors, initially, in private<br>(Note: This category is not appropriate to a document that could be categorised in some other way | OFFICIAL-SENSITIVE: COMMERCIAL |
| Commercial | Where disclosure would be likely to damage a (third party) commercial undertaking's processes or affairs except subject to the FOI Act. | OFFICIAL-SENSITIVE: COMMERCIAL |
| Contracts | Concerning tenders under consideration and the terms of tenders accepted | OFFICIAL-SENSITIVE: COMMERCIAL |
| Management | Concerning policy and planning affecting the interests of groups of staff (Note: Likely to be exempt only in respect of some health and safety issues) | OFFICIAL-SENSITIVE: COMMERCIAL |
| Patient Information | Concerning identifiable information about patients | OFFICIAL-SENSITIVE: PERSONAL |

| | | |
|---|---|---|
| Personal | Concerning matters personal to the sender and/or recipient | OFFICIAL-SENSITIVE: PERSONAL |
| Proceedings | The information is (or may become) the subject of, or concerned in a legal action or investigation. | OFFICIAL-SENSITIVE: COMMERCIAL |
| Staff | Concerning identifiable information about staff | OFFICIAL-SENSITIVE: PERSONAL |

# Corporate Documentation Management (Information Lifecycle) 2015
#NGH-P0-123

**Area of Work**
Strategy & Partnerships

**Person Responsible**
Sarah Kinsella

**Created**
26th June, 2015

**Last Review**
26th June, 2015

**Status**
Complete

**Next Review**
31st July, 2016

## Screening Data

What is the name, job title and department of the lead for this procedural document?

Kehinde Okesola,Information Governance Manager, Information Governance

What are the main aims, objectives or purpose of this procedural document?

The purpose of this policy is to ensure a consistent and effective approach to the management of all documentation within the Trust by:
â€¢Defining the role of documentation management within the Trust
â€¢Â Identifying roles and responsibilities for documentation management
â€¢Â Providing guidance on meeting legal and professional requirements for documentation management
â€¢Â Detailing the standard to be followed for the transportation, transmission and secure storage of documentation; especially where these documentation contain person identifiable information (PID).
â€¢Â Setting out Trust retention periods for all types of documentation
â€¢Â Indicating how compliance with this policy will be monitored and maintained

Who is intended to benefit from this procedural document?

This policy applies to everyone working at Northampton General Hospital NHS Trust who has any interaction with documentation, including, but not limited to, permanent staff, temporary staff, students, locums, volunteers, researchers and staff on honorary contracts (all referred to as 'staff' in this document).
For the purpose of this policy, documentation are defined as: recorded information irrespective of format, which is created, received and maintained by the Trust in the execution of its business.
This policy covers all documentation, in all formats, both active and inactive, held for use in NGH, including but not limited to:
â€¢Â Non-clinical e.g. administrative, corporate, personnel, estates, finance and litigation, including emails and text messages
This policy excludes all documentation created by other organisations, such as the Department of Health, which are kept for reference and information only, unless they include person identifiable information.
It is important to note that this policy does not replace any existing policies, but works in conjunction with them where indicated. It provides a high-level overview, which sets out the connections between the various Trust policies that contribute towards the management of all Trust documentation of staff, its departments, business operations and activities.

Is this a Trustwide, Directorate only or Department only procedural document?

Trustwide

Is there potential for, or evidence that, this procedural document will not promote equality of opportunity for all or promote good relations between different groups?

No

Is there potential for, or evidence that, this proposed procedural document will affect different protected groups/characteristics differently (including possibly discriminating against certain groups/protected characteristics - see below)?

Age

Disability

Gender Reassignment

Marriage & Civil Partnership

Pregnancy & Maternity

Race

Religion or Belief

Sex

Sexual Orientation

No

If the answer to one or both of the questions above is 'yes', the full Equality Analysis process must be undertaken.

If the answer to both of the questions above is 'no' then the full Equality Analysis process is not required and the Organisational Sign-Off can be now be completed.

Based on the answers given, to the questions above, is a full Equality Analysis required?

No

### Recommend this EA for Full Analysis?

No

### Rate this EA

Low

## Organisation Sign-off Data

Do you have any recommended actions?

If you have made any recommended actions have you advised the procedural document lead of these?

N/A

### Comments

Consideration should be given to ensuring that this document is made available in alternative formats to enable access for staff who may be not be able to access it in its current format.

### Next Review Date

2016-07-31

## Outstanding Actions

No outstanding actions

FORM 1 & 2 - To be completed by document lead

| **FORM 1a- RATIFICATION FORM - FOR COMPLETION BY DOCUMENT LEAD**<br>Note: Delegated ratification groups may use alternative ratification documents approved by the procedural document groups. | |
|---|---|
| **DOCUMENT DETAILS** | |
| Document Name: | Corporate Documentation Management (Information Lifecycle) NGH-P0-123 |
| Is the document new? | No |
| If yes a new number will be allocated by Governance | N/A |
| If No - quote old Document Reference Number | NGH-PO-123 |
| This Version Number: | **Version: 3.1** |
| Date originally ratified: | |
| Date reviewed: | June 2015 |
| Date of next review: a 3 year date will be given unless you specify different | **June 2018 (3 Years)** |
| If a Policy has the document been Equality & Diversity Impact Assessed? (please attach the electronic copy) | Yes / No |
| **DETAILS OF NOMINATED LEAD** | |
| Full Name: | Kehinde Okesola |
| Job Title: | Information Governance Manager |
| Directorate: | Strategy and Partnerships |
| Email Address: | Kehinde.okesola@ngh.nhs.uk |
| Ext No: | 3881 |
| **DOCUMENT IDENTIFICATION** | |
| Keywords: **please give up to 10** – to assist a search on intranet | Records, retention, confidential disposal, destruction, data, confidentiality, information, personal information, Legal Compliance |

**GROUPS WHO THIS DOCUMENT WILL AFFECT?**
**( please highlight the Directorates below who will need to take note of this updated / new Document )**

| | | |
|---|---|---|
| Anaesthetics & Critical Care | General Medicine & Emergency Care | Medical Physics |
| Child Health | Gynaecology | Nursing & Patient Services |
| Corporate Affairs | Haematology & Oncology | Obstetrics |
| Diagnostics | Head & Neck | Ophthalmology |
| Estates & Facilities | Human Resources | Planning & Development |
| Finance | Infection Control | Trauma & Orthopaedics |
| General Surgery | Information Governance | **Trust Wide** |

TO BE DISSEMINATED TO: NB – **if Trust wide document it should be electronically disseminated to Head Nurses/ Dm's and CD's .List below all additional ways you as document lead intend to implement this policy such as; as presentations at groups, forums, meetings, workshops, The Point, Insight, newsletters, training etc below:**

| Where | When | Who |
|---|---|---|
| Training | Mandatory Training and Induction | All staff |

FORM 1 & 2 - To be completed by document lead

| | | |
|---|---|---|
| Presentations | As and when scheduled | Target staff groups |

**FORM 2 - RATIFICATION FORM to be completed by the document lead**

**Please Note:** Document will not be uploaded onto the intranet without completion of this form

**CONSULTATION PROCESS**

*NB: You MUST request and record a response from those you consult, even if their response requires no changes. Consider* Relevant staff groups that the document affects/ will be used by, Directorate Managers, Head of Department ,CDs, Head Nurses , NGH library regarding References made, Staff Side (Unions), HR Others please specify

| Name, Committee or Group Consulted | Date Policy Sent for Consultation | Amendments requested? | Amendments Made - Comments |
|---|---|---|---|
| Julie Quincey - Safeguarding Children | 21 January 2015 | None | |
| Elizabeth Tee- Oncology | 21 January 2015 | I can find no reference to Clinical Trials/Research documents in the Lifecycle policy, it may be covered under policies but I wonder if it needs to be included | Noted. Liaised with Julie Wilson |
| Julie Wilson – R&D | 21 January 2015 | There is a raft of records management that refer to research<br><br>I think the best way of handling this is rather than to itemise things – to encompass all research and refer the reader to the Records management code of practice Part 2 from page 55 | Research and Development Record Retention Schedule included. |
| Fiona Barnes - Patient & Nursing Services | 21 January 2015 | None | |

**Existing document only - FOR COMPLETION BY DOCUMENT LEAD**

| | | |
|---|---|---|
| Have there been any significant changes to this document? *if no you do not need to complete a consultation process* | | YES / NO |
| **Sections Amended:** | YES / NO | **Specific area amended within this section** |
| Re-formatted into current Trust format | YES / NO | |
| Summary/ Introduction/Purpose | YES / NO | |
| Scope | YES / NO | |
| Definitions | YES / NO | |
| **Roles and responsibilities** | YES / NO | |
| **Substantive content** | YES / NO | **Sharing of information for safeguarding purposes** |
| **Monitoring** | YES / NO | |
| Refs & Assoc Docs | YES / NO | **Addition of the safeguarding children policy** |
| Appendices | YES / NO | **Addition of the key retention Schedules and Protective Marking Scheme (New Government Security Classifications – published April 2014)** |

| **FORM 3- RATIFICATION FORM** (FOR PROCEDURAL DOCUMENTS GROUP USE ONLY)<br>**Read in conjunction with FORM 2** | | | |
|---|---|---|---|
| **Document Name:** | **Information Lifecycle v2** | **Document No:** | **NGH-PO-123** |
| **Overall Comments from PDG** | | | |

| | **YES / NO / NA** | **Recommendations** | **Recommendations completed** |
|---|---|---|---|
| **Consultation** Do you feel that a reasonable attempt has been made to ensure relevant expertise has been used? | **YES / NO / NA** | | |
| **Title** -Is the title clear and unambiguous? | **YES / NO / NA** | | |
| Is it clear whether the document is a strategy, policy, protocol, guideline or standard? | **YES / NO / NA** | | |
| **Summary** Is it brief and to the point? | **YES / NO / NA** | | |
| **Introduction** Is it brief and to the point? | **YES / NO / NA** | | |
| **Purpose** Is the purpose for the development of the document clearly stated? | **YES / NO / NA** | | |
| **Scope** -Is the target audience clear and unambiguous? | **YES / NO / NA** | | |
| **Compliance statements –** Is it the latest version? | **YES / NO / NA** | | |
| **Definitions** –is it clear what definitions have been used in the | **YES / NO / NA** | Amend FoiA to Capitals FOIA | |
| **Roles & Responsibilities** Do the individuals listed understand about their role in managing and implementing the policy? | **YES / NO / NA** | | |
| **Substantive Content** is the Information presented clear/concise and sufficient? | **YES / NO / NA** | | |
| **Implementation & Training** – is it clear how this will procedural document will be implemented and what training is required? | **YES / NO / NA** | | |
| **Monitoring & Review** (policy only) -Are you satisfied that the information given will in fact monitor compliance with the policy? | **YES / NO / NA** | | |
| **References & Associated Documentation** / **Appendices**- are these up to date and in Harvard Format? Does the information provide provide a clear evidence base? | **YES / NO / NA** | | |
| **Are the keywords relevant** | **YES / NO / NA** | | |

| **Name of Ratification Group:**<br><br>**PDG** | **Ratified Yes/No:**<br><br>**Comments:** | **Date of Meeting:**<br><br>**16/04/2015** |
|---|---|---|