Corporate Records Management Guidance

Issue Sheet

<table>
<thead>
<tr>
<th>Document reference</th>
<th>NHSBSARM015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document location</td>
<td>S:\BDA\IGM\Managing IG\Providing Advice and Training\RM Advice and Guidance\00 Final and Current\NHSBSARM015 RM Guidance</td>
</tr>
<tr>
<td>Title</td>
<td>NHSBSA Corporate Records Management Guidance</td>
</tr>
<tr>
<td>Author</td>
<td>Rachel Hardiman / Records Manager</td>
</tr>
<tr>
<td>Issued to</td>
<td>All staff</td>
</tr>
<tr>
<td>Why issued</td>
<td>Information / Action</td>
</tr>
</tbody>
</table>

Revision Details

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Amended by</th>
<th>Approved by</th>
<th>Details of amendments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>02 Feb 2011</td>
<td>IGSG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.0</td>
<td>17 Mar 2011</td>
<td>Rachel Hardiman</td>
<td>n/a</td>
<td>Minor change to Section 6.1.2.7 on versioning to align RM guidance with PMO practice.</td>
</tr>
<tr>
<td>3.0</td>
<td>31 Mar 2015</td>
<td>C Gooday</td>
<td>RMF</td>
<td>Remove references to GroupWise in section 7.2 bullet 9</td>
</tr>
<tr>
<td>4.0</td>
<td>21 Mar 2016</td>
<td>C Gooday</td>
<td>RMF</td>
<td>Annual Review 6.4.3 added HSCIC guidance link on destruction</td>
</tr>
<tr>
<td>5.0</td>
<td>14 Oct 2016</td>
<td>C Gooday</td>
<td>RMF</td>
<td>Reflect change to Government Classification</td>
</tr>
</tbody>
</table>
Contents

CONTENTS ......................................................................................................................... 2

PART A ................................................................................................................................. 3

2.1 What are Records? .............................................................................................................. 3
  2.1.1 What are Business Records? .................................................................................... 3
  2.1.2 The elements of a record .......................................................................................... 3
  2.1.3 Examples of Records ............................................................................................... 4
    2.1.3.1 Official records .................................................................................................. 4
    2.1.3.2 Records created in everyday activities using office or desktop software packages ........................................................................................................... 5
    2.1.3.3 Records created in line-of-business or support systems and databases, common examples of which are ................................................................................. 5
    2.1.3.4 e-Mails, instant messages, or other forms of electronic communication that document or discuss: .............................................................................................. 5
  2.1.4 Transitory records: ..................................................................................................... 6
  2.2 Information owned by the NHSBSA ............................................................................... 7
  2.2.1 Information owned by third parties but stored or hosted by NHSBSA ....................... 7
  3.1 What is Recordkeeping? ............................................................................................... 8
  3.2 When to create a record ............................................................................................... 9
  3.2.1 When to create a record .......................................................................................... 9
  3.2.2 What to call a record ............................................................................................. 9
  3.2.3 Where to keep records ........................................................................................... 9
  3.2.4 How to keep records ............................................................................................. 9
  3.2.5 How long to keep records ...................................................................................... 10
  3.2.6 How to dispose of records .................................................................................... 10
  3.2.7 Records as evidence .............................................................................................. 10
  3.2.8 Access to records .................................................................................................. 10
  3.2.9 Sustainability ......................................................................................................... 11
  4.1.1 Retention is format-independent ............................................................................ 13
  4.1.2 Mandates for retention periods .............................................................................. 13
  4.1.3 Some terms used in the Retention Schedule .......................................................... 13
    4.1.3.1 Substantive Records / Correspondence .............................................................. 13
    4.1.3.2 Administrative Records / Correspondence ....................................................... 14
    4.1.3.3 Transitory Records .......................................................................................... 14
    4.1.3.4 Drafts and Versions ......................................................................................... 14
  4.1.4 Implementing disposal of records ............................................................................ 14
    4.1.4.1 Destruction of records ..................................................................................... 14
    4.1.4.2 Litigation Holds .............................................................................................. 14
    4.1.4.3 Long-term retention ....................................................................................... 14
    4.1.4.4 Closure period ............................................................................................... 15
  5.2.1 Model File-plan ....................................................................................................... 17
    5.2.1.1 Assigning retention details to folders .............................................................. 17
    5.2.1.2 Reference material ........................................................................................ 18

PART B ................................................................................................................................ 19

6.1 When to create a record ............................................................................................... 19
  6.1.1 Use the corporate file-plan to structure your files .................................................... 21
    6.1.2.1 Structure files to support the Retention Schedule ............................................. 21
    6.1.2.2 File names should be short, but meaningful ....................................................... 21
    6.1.2.3 Avoid repetition when naming sub-folders ....................................................... 21
    6.1.2.4 Avoid using non-alphanumeric characters in file titles .................................. 22
    6.1.2.5 Add the date of creation to the file title ............................................................ 22
  6.1.2.6 If the date or identifier is part of the file or record title, always make it the first part of the file name .................................................................................................... 22
  6.1.2.7 The version number of a record should, where applicable, be included .............. 22
  6.1.2.8 Use only agreed abbreviations ........................................................................... 23
  6.2 The role of guidance and Standard Operating Procedures (SOPs) ............................... 23
  6.2.1 Filing a record on creation ...................................................................................... 23
1 Overview

This document is intended to provide more detailed guidance on implementing the NHSBSA’s records management strategy and policy, using tools such as the Retention Schedule (NHSBSARM012) and Business Classification Scheme (NHSBSARM014) along with standard or best-practice principles and methods of records management and recordkeeping.

Responsibility for implementing the strategy and policy lies partly with the central Records Management function, and partly with each member of staff who creates, receives, or uses records and other information related to the business activities of the NHSBSA. In general, primary responsibility for records management lies with the former, and for recordkeeping, with the latter.

These guidelines and the various other NHSBSA records management referenced within them have been drawn up to assist local records managers and other staff to fulfil their records management responsibilities. They will be incrementally and regularly updated until they are of sufficient scope and complexity to fully comply with the terms of the NHSBSA’s Records Management Policy, after which they will be reviewed on a regular basis to ensure that they continue to meet requirements.

Records Management is a framework that supports responsible decision-making about the records – or evidence – of an organisation’s business activity. Recordkeeping is a term used for transactional, or local, records management activity; that is, recordkeeping is what staff do every day with the documents and records that they create in the course of their work. Recordkeeping should be supported by local documentation and training, derived from that provided by central Records Management.

The document is split into three parts:

- Introductory sections on concepts and tools
  - the concept of records
  - the concept of records management
  - NHSBSA Retention Schedule
  - NHSBSA Business Classification Scheme.
- Guidance specific to keeping and managing records within the context of the NHSBSA
- Guidance on topics related to, or having an impact on, keeping and managing records
  - e-mail management guidance

Throughout this document, references to other resources, internal or external, are either given in a footnote or highlighted within the body of the text by appearing in blue. Full details of these resources and their associated hyperlinks, where applicable, are given in Appendix 1.

Further resources on records management and recordkeeping, both internal and external, are given in Appendix 1, and are also mentioned throughout this document wherever they are particularly appropriate. A glossary of the records management

---

1 NHSBSARM002 NHS Business Services Authority Records Management Strategy
2 NHSBSARM001 NHS Business Services Authority Records Management Policy
terms used in this document and the various other tools and documents to which it relates is included in Appendix 2.
2 An Introduction to records

2.1 What are Records?

Any type of recorded information, regardless of physical form or characteristics, created, received, or maintained by a person, institution, or organization… Records are extensions of the human memory, purposefully created to record information, document transactions, communicate thoughts, substantiate claims, advance explanations, offer justifications, and provide lasting evidence of events. Their creation results from a fundamental human need to create and store information, to retrieve and transmit it, and to establish tangible connections with the past.³

2.1.1 What are Business Records?

Records include all books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency [in accordance with its legal obligations] or in connection with the transaction of … business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the [agency] or because of the informational value in them.⁴

More succinctly, business records are

Information created, received, and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business.⁵

For the purposes of recordkeeping and records management in the NHSBSA, we are concerned with Business Records. However, not all records are of equal standing: some – generally described as ‘Transitory Records’ – are of only temporary or ephemeral value, and do not need to be managed with the same level of rigour, or kept for the same length of time, as other records.

Of the remaining records – those that do need to be maintained and managed according to recognised standards and best practice – some have more stringent requirements than others: for instance, access and security settings will apply to certain classes of records, while others need to be kept for such a long period that special measures need to be in place to ensure that they remain usable and accessible over time.

2.1.2 The elements of a record

A record, or any other piece of information, has two fundamental elements – content and structure. In practice, the two may not be rigidly separated: for instance, the address, salutation, and signature in a formal letter are both content (e.g., they tell you who it is that wrote the letter) and structure (regardless of the content, they tell you that this document is a letter, that it has been addressed to someone and sent by someone).

⁴ 44 U.S.C. Chapter 33, Sec. 3301
⁵ BS ISO 15489-1:2001 Information and documentation — Records management — Part 1: General, Sect. 3.15
Many of the structural aspects of a record are found in its metadata, literally ‘data about data’. Apart from the sort of ‘structural content’ described in the previous paragraph, metadata most commonly take the form of file names and dates, tags, field names, contextual positioning, etc.

So, for instance, a paper file will be contained in a folder on which may be written a folder name, a date or date range, a topic, a reference code, a department name, a filing location, or any other of the types of marking commonly found on folders. An electronic file, too, may be contained in a folder, or data in a field in a database; additional information such as date of creation, date last viewed, author, size of file, details of software version, etc may be added automatically or amended manually. All of these are examples of metadata.

A record is not generally accessible or usable without certain basic metadata, such as a file or document name. Or it may be accessible, yet unreliable or incomplete: if, for instance, a letter has been sent but the name of the sender is not included, or (as often happens) an electronic template is used without amending the existing metadata so that, e.g., the author name in the document properties is not that of the actual author.

Much good practice in records management and recordkeeping is concerned with creating and maintaining good metadata: any structuring tool or framework, such as a file-plan, is a form of metadata; and conventions about file names, version control, colour-coding paper files, adding security flags, etc is all aimed at ensuring that appropriate metadata is created and captured.

### 2.1.3 Examples of Records

Here are some of the forms that records may take in the NHSBSA or any other organisation:

- official records, essential to the ongoing business of the BSA. For example, registered files, official minutes, regulations, agreements, legal records and financial records, which affect or define the BSA’s functions and activities
- records of business activity required to be retained by the corporate retention schedule, whether for immediate business purposes or because their retention is required by UK, European or international law.
- records containing essential information of the rights and obligations of the BSA or of any other persons.
- information likely to be required for the determination of any action in any inquiry, court or tribunal.
- material of significance or public interest.
- client records, case files, project files, personnel records, development of policy issues

Records can be in any format, ranging from traditional hard-copy files to on-line social networking tools (although, naturally, not all types of record will be in use within the BSA or any other organisation). It is the content and business context of an item that determines whether it is a record. Some common types of record found in most offices are:

#### 2.1.3.1 Official records

- case file information
• invoices
• contracts
• meeting notices
• completed forms
• correspondence – internal and external
• policy directives and related communications
• faxes
• applications
• reports
• decision papers
• databases

2.1.3.2 Records created in everyday activities using office or desktop software packages
• policy or procedures
• frequently asked questions (FAQs) publicised on corporate intranet and internet sites
• project documentation
• minutes and reports
• correspondence that requires action from recipients
• Excel spreadsheets that contain formulas needed to substantiate financial transactions
• Visio diagrams, e.g., that document processes or workflow, organizational charts
• PowerPoint presentations, if they contain original material not documented elsewhere or if they constitute evidence of activities such as training or briefing
• AutoCad and other designs and modelling
• completed forms

2.1.3.3 Records created in line-of-business or support systems and databases, common examples of which are
• HR systems
• Finance and payroll systems
• GIS systems
• Internets and intranets
• CRM (customer relationship management) systems

2.1.3.4 e-Mails, instant messages, or other forms of electronic communication that document or discuss:
• policy and decisions – their creation and actions for implementation
• client/customer communications
• staff assignments
• information which protects the financial, legal, and other rights of the BSA and of persons directly affected by its actions
e-Mail is often thought of as an informal communication medium, and e-mail messages as informal documents that do not have the status of records. *This is not the case.* If an e-mail relates to the conduct of the BSA’s internal or external business, it is every bit as much a record as a formally signed and sealed contract or deed. Because the informality of the medium gives rise to a huge ‘sprawl’ of e-mails, many relatively trivial mails that nonetheless are records must be managed in full compliance with the BSA’s records management policies and procedures. Advice is available in Section 7 to help minimise the number of e-mails generated for business purposes.

2.1.4 Transitory records:

- routine material that facilitates day-to-day operations but does not set policy, establish guidelines or procedures, certify a transaction or become a receipt
- documents of short-term interest, used for reference, with no evidentiary value
- duplicate copies of documents preserved only for convenience; materials not filed as evidence of business unit/service operations or for their informative value
- modifications and updating of data as part of the running of established electronic software programmes, where such processes do not result in the loss of data of continuing value.
- rough notes, calculations or non-substantive drafts created to prepare or analyse other documents
- background materials used to develop a record
- documents or communications that are not needed for the official record, but are useful to an individual for recall of events, activities, and actions.

Transitory records can be deleted after the immediate context for their use has passed; a reasonable retention period is three months after the action that they supported ceased. It is important, however, to remember that they are still records – they should be created and maintained as systematically as other, more long-term records and kept in the same formal shared recordkeeping environments. They should not be squirreled away on personal hard drives or, if they are paper-based, left forgotten in drawers and cabinets. It is especially important to ensure that any duplicates of other BSA records made for reference purposes are deleted in a timely fashion. If they are not, they may continue to exist after the ‘master’ record has been scheduled for deletion or other action, and cause the BSA to be in dereliction of its information governance and legal obligations.

If certain materials, whether internal or external, are frequently copied and re-used as reference sources (e.g. a Department of Health leaflet, a previous letter or report used as a model for drafting a new one), consider maintaining a ‘reference library’ folder or drafting templates with boiler-plate text to form a continuing shared repository for these items.

*n.b.* Although reference material should be disposed of or centralised, it may be necessary, depending on the record being created, to maintain an audit trail of material consulted by providing references within the resulting record. For instance, a report that draws on previous legislation, guidance, or other publications should cite the sources used, which helps fulfill transparency and audit requirements and also serves to underscore the authority of the views or facts included.
2.2 What is not a Record?

2.2.1 Information owned by the NHSBSA

Not all recorded information is a business record, since it has not been produced or received in the conduct of business. These include:

- stocks of printed or reproduced documents kept for supply purposes where master copies have been retained for record purposes.
- books, periodicals, newspapers, or other materials kept for reference purposes.
- personal materials which have no relation to official duties, including e-mails such as “are you going on lunch?” and all-staff social announcements, such as birthday celebrations or charity campaign notices.

Printed publications are not records if they originate from external sources; however, records of publications actually issued by the BSA should include two reference hard copies (along with the electronic master or authorised copy, if relevant) of each publication, to be kept in the long term for archival purposes and as business evidence, after other surplus copies have been disposed of when their purpose has been served. In the absence of a corporate library or information centre, this will be the responsibility of the department or group that published them.

2.2.1 Information owned by third parties but stored or hosted by NHSBSA

Some of the recorded information held by the BSA belongs to third parties and has no connection with the business of the BSA. For instance, the BSA provides server space and computer facilities to Trade Union representatives, but the information stored are the records of the Trade Union rather than the BSA.

2.3 Is it a Record? Short Checklist

Finally, a quick though non-exhaustive checklist that may help in deciding whether something is or is not a record …

- Does it record a business activity or event?
- Do you need it to prove a transaction did – or did not – occur?
- Do auditors require you to retain it?
- Could it be used to resolve a dispute in the future?
- Do you need it to identify who participated in an event or had knowledge of an event?
- Does it support facts you claim to be true (if the person with direct knowledge of the facts has retired or is otherwise unavailable)
- Does it support what you do?
  - Communicate with a client?
  - Document activities regarding a particular matter?
- Does it have business, legal or historical value?

Further information in respect of this section or the document as a whole is available from the corporate Records Manager. Background information and supporting guidance on this section can be also found in resources such as the ISO Records Management standard BS ISO 15489-1:2001. The Wisconsin Department of Administration has produced a good and user-friendly presentation on Records Management Basics, on which some of this section has been based.
3 A Brief Introduction to Records Management

This section is intended to guide all staff as to when they should expect to consider records management issues in relation to their own job. It is intended also to act as a reminder that the management of records is not an activity that is separate from everyday activity, but should be integrated into routine business activities.

More detailed guidance about records management in the NHSBSA is contained in the Business Rules.6

3.1 What is Records Management?
The nature and characteristics of records have been described in Section 2. Records Management is a framework that supports responsible decision-making about the records – or evidence – of an organisation’s business activity. There is no single system that can be deployed in every organisation and no single set of rules that define exactly how to address each records-related procedure. Instead, records management has to be developed in the specific context in which it is to be practised, in order that it can mesh as closely as possible with the organisation’s everyday activity. It is a flexible framework, embedded in the organisation’s administrative routines, that can be adapted as business needs or responsibilities change.

The records management framework is developed by comparing the records of business activity with external standards for records, best practice for management of records, and legislation which affects records. So before an organisation can introduce records management, it must investigate and document what exactly each part of the organisation does, how that activity is recorded, how that record is subsequently used, and what are the legal obligations in relation to it.

Records Management is part of the wider information activities of an organisation. It will support:

- good decision-making
- effective business performance
- effective management of resources such as staff time and physical or server space
- audit
- compliance with information legislation
- corporate memory

3.1.1 What is Recordkeeping?
Recordkeeping is a term that can be used to describe the act of making and keeping records in the broadest terms. However, it is also used in a more specific sense (which applies here) as indicating transactional, or local, records management; that is, recordkeeping is what staff do every day with the documents and records that they create in the course of their work. Recordkeeping should be supported by local documentation and training, derived from that provided by central Records Management.

3.2 Records Management and Recordkeeping Responsibilities
The principal requirements and responsibilities in relation to managing the NHSBSA’s records are outlined below. Some of these areas are treated in greater detail in other sections of this guidance.

6 NHSBSARM009 Business Rules for Creation, Management and Disposal of Records on behalf of the NHSBSA
3.2.1 When to create a record

In the majority of cases, there will be little ambiguity about when to create records, as the business process will be such that recording the evidence of the activity will arise organically. However, in some instances it may be a separate activity. The NHSBSA Business Rules lay out guidelines as to what should be recorded.

It is important to remember when not to create a record. This, too, is dealt with in the Business Rules and is also connected with our responsibilities under the Data Protection and the Freedom of Information Acts.

Finally, it is important to remember that some information is more sensitive than others. This is particularly important with regard to personal information about living individuals, especially if the information is sensitive (e.g., related to race, religion, medical history, etc). Be sure that this is only collected where it is absolutely needed and that it is disposed of at the earliest appropriate opportunity. See Information Governance guidance on the Data Protection Act for further advice.

3.2.2 What to call a record

A record should be given a name that will make sense to other people, and that will facilitate locating the record once it is no longer in use. Never use your own name, or terms such as ‘Miscellaneous’, as file or document names. Avoid using subject phrases (e.g., “Procedures Manual”) as a file title, but include a verb to indicate the business activity (e.g., “Producing Records Management Procedures Manual”).

Further guidance on naming conventions for files, folders, and documents are given in Section 6.1.2.

3.2.3 Where to keep records

The model Corporate File-plan should be used as a basis for decisions about locating records, both physically and conceptually. The aim of the file plan is to encourage standardised recordkeeping across the NHSBSA, particularly in those functions and activities (e.g. line-managing staff, managing projects, meetings) which are common to all business areas. Additional requirements will apply to records – physical or digital – which have a security requirement (e.g., knowledge of the contents or even the existence of certain files may need to be limited to certain staff).

Records should never be kept ‘outside the system’ (e.g. on PC hard drives, on CDs or other removable media) except as temporary off-site copies driven by a business need to work off-site or off-line. Such records, whether originals or copies, compromise the NHSBSA’s ability to account for the information it holds and the way in which that information is used and managed.

3.2.4 How to keep records

Where there is a high volume of records it may make operational sense to consider scanning the paper and then disposing of it, retaining the image instead. If this is a possibility then there are records management requirements both in terms of the result of the scanning (legal admissibility) and also for retention (digital preservation). This approach also depends on there being sufficient storage capacity on the BSA’s networked servers.

It is also common for staff to keep both hard-copy and electronic versions of files. This should be avoided, as it is unnecessary duplication and may undermine the

---

7 An Introduction to Data Protection, freedom of Information & Information Security for Employees
reliability of the record (if the files are not exact copies of each other). In general, there should be no unplanned redundancy in the recordkeeping systems, though it is not only legitimate but desirable – in the case of vital records, essential – to keep managed back-up copies of records for business continuity and preservation purposes (see Section 8).

3.2.5 How long to keep records
The reasons for keeping records will be based on legislative requirement, business need or best professional practice. The Corporate Retention Schedule\(^8\) outlines the retention periods for different classes of record and there should be no local variation on this without central agreement.

3.2.6 How to dispose of records
The majority of records can be disposed of in a straightforward manner, by shredding or recycling, though if the record is sensitive (e.g., it contains personal information) then it may need to be disposed of with greater care. It is important to remember that if the record is due for disposal, all copies must be disposed of, including those contained on removable media (e.g., CDs).

It is important to remember that simply ‘deleting’ a digital file from a server or hard drive does not destroy it: the record must be destroyed beyond any possibility of reconstruction. This applies whether or not the record is scheduled for secure destruction. Remember that most modern scanners, photocopiers, fax machines etc store cached copies of the documents they process – these cached copies should be purged regularly.

Where secure destruction of paper records is mandated, suitable arrangements must be made with Estates to ensure that this is carried out in a controlled manner and the appropriate sign-off and certification obtained.

Further information on disposing of records is available in Section 6.4.

3.2.7 Records as evidence
Records demonstrate how an organisation performs its business activities. Sometimes records will be required as evidence in litigation. In such instances, it is important that the record be available (that it can be identified, located and is not stored on media so old that it cannot be opened) and reliable. There may be occasions where litigation has started but where records that might be required are due for destruction. In this case, a litigation hold may be placed on the record, which means that the normal retention period should not be applied.

3.2.8 Access to records
The NHSBSA aims to be as open and transparent as it can be, and takes the view that information should be available, internally and externally, unless there is a specific reason to withhold it. The organisation’s compliance with the requirements of the Data Protection Act and the Freedom of Information Act is managed by Information Governance. However, individual members of staff are responsible for ensuring that they do not permit unauthorised access to records in their custody. This requirement applies to both electronic records and to paper records. Guidance and training is available from Information Governance.

---

\(^8\) NHSBSARM012 NHSBSA Corporate Records Retention Schedule
3.2.9 Sustainability
The NHSBSA has an environmental responsibility and has undertaken to try and ensure that its practices are environmentally sustainable. This will include, for example, staff avoiding creating paper records unless it is necessary and minimising duplication.

Further information can be found in numerous sources; two good examples from the UK are JISC InfoNet's Records and Information Management web pages and the parts of Staffordshire County Council's Records Management Manual that deal with record management in general.
4 An Introduction to the NHSBSA’s Corporate Retention Schedule

A retention schedule, also called a disposal schedule, is an agreed schedule of how long records are to be retained. It is usually based on a mixture of legal requirement and best practice – for example, the Companies Act 1980 requires retention of financial records for 6 years after the end of the current financial year but there is no legislation about how long to retain the application forms of unsuccessful job applicants. Therefore organisations make some decisions for themselves. Additionally, it may be operationally more appropriate to apply the retention schedule at file rather than document level, even if this means that some records within the file are retained for longer than recommended. It is important that this fact is recorded, e.g., in SOPs (Standard Operating Procedures).

Each business area will have a local retention schedule derived from the Corporate Retention Schedule. It is important to remember that both local schedules and the corporate schedule are live documents and need to be maintained in conjunction with each other. Any changes to the corporate schedule should be reflected in the relevant local schedule(s). Equally importantly, any new local requirements must be discussed centrally first, and only added to a local schedule when agreement is reached. In this way, the corporate schedule remains relevant to the business as a whole, and reflects the NHSBSA’s changing needs in a structured and sustainable way.

Until more formal mechanisms are put in place, changes or change requirements are communicated on an ad hoc basis by e-mail and discussion between the corporate records Manager and staff with local records management responsibilities.

The aims of the schedule and associated guidance are to:

- assist in identifying records that may be worth preserving permanently as part of local or national archives
- prevent the premature destruction of records that need to be retained for a specified period to satisfy legal, financial and other requirements of public administration
- provide consistency for the destruction of those records not required permanently after specified periods
- promote improved Records Management practices within the NHSBSA

The functions and activities by which the Retention Schedule is organised are derived from the Business Classification Scheme (see Section 5).

4.1 Using the Retention Schedule

It is very important that records are not destroyed earlier than the length of time specified in the retention schedule; the schedule always gives the minimum period of time and this should not be deviated from without explanation and agreement in writing.

The retention period starts when a file is closed or otherwise finalised – e.g., the retention period of 6 years applicable to a non-sealed contract takes effect from the date on which the contract expires, not the date from which it is effective. The only exception is for transitory records, where retention is calculated from the date they cease to be needed for the activity they supported – frequently, the date on which that activity started or became definitive.
For this reason, it is important to organise records, whether digital or non-digital, in file and folder structures that support the implementation of the Retention Schedule. For example, one of the activities of line-managing staff is conducting appraisal; substantive records of each year’s appraisal are scheduled to be kept for six years. It is therefore not enough to have all of an individual’s appraisal records held in a single file called ‘Bloggs J’, or even to separate them out in a folder called ‘Bloggs J Appraisals’ – there will need to be sub-divisions for each year, so that each year’s appraisal records can be disposed of in turn when six years have passed. Or, using a different structure, disposal actions might be applied to a folder called ‘2009 Appraisals’ and all of its sub-folders ‘Bloggs J’, ‘Other A N’, etc.

In digital files on a networked drive, this can be achieved by having sufficient levels of subfolders. A similar approach applies to paper files, except that where the number of documents is low, it is sufficient to create virtual ‘sub-folders’ by using internal dividers in a single physical folder to separate out the records to which the same disposal date applies – what matters is that the relevant records can be easily identified as a group rather than by having to search through the whole file.

4.1.1 Retention is format-independent

Retention and disposal requirements are independent of any particular format of record that might be historically created (e.g. card, register) or media (e.g. paper, electronic). All records management documentation focuses on the record as a product of an activity, rather than as part of a subject-based group, or the product of a particular administrative division, or as captured in certain forms or on certain media. This helps to make records management guidance and procedures flexible, and to prolong their period of application, since they are less likely to be invalidated by changes in processes or technology.

4.1.2 Mandates for retention periods

The retention periods identified in the retention schedule are based in the first instance on the NHS Records Management Code of Practice (the CoP). Where the CoP does not include records produced by the NHSBSA, the retention period will have been informed by guidance from The National Archives, information advisory bodies (e.g., Joint Information Systems Committee (JISC)), large national organisations whose records management practice has been publicly recognised as having a high professional standard (e.g., Universities of Edinburgh and of Glasgow) or developed from business need within the NHSBSA.

4.1.3 Some terms used in the Retention Schedule

4.1.3.1 Substantive Records / Correspondence

The term ‘substantive’ covers documents, letters, memos, e-mails etc whose content contains significant information, such as a decisions, comments, instructions, approval or rejection, etc. Note that a short e-mail or even a signed sticky note saying ‘Yes, this is OK’ is substantive if it constitutes the only explicit decision or instruction on a given matter. Generally, substantive correspondence is retained for the same period as the primary document or item to which it relates.
4.1.3.2 Administrative Records / Correspondence
The term ‘administrative’ in this context covers documents, letters, memos, e-mails etc whose content contains non-trivial but less significant information relating to the administration or organisation of business activities, meetings, events, information-gathering, etc.

4.1.3.3 Transitory Records
Records of merely temporary or ephemeral value, such as purely facilitative routine material, duplicates preserved only for convenience, documents used for reference, background materials used to develop a record, etc.

Further details of the types of record considered transitory can be found in Section 2.1.4.

4.1.3.4 Drafts and Versions
These two terms have distinct meanings and different retention requirements. A draft is a work in progress, which has not yet been signed off or reached stable form. Drafts are still records, and where there is significant variation between drafts, they can be considered substantive. A version is a stable manifestation of a record subject to change over time, which constitutes the definitive record until superseded. Since the term ‘version’ is often applied to different draft stages, the file name of draft records should always include the word ‘Draft’ to differentiate it from approved, stable versions.

4.1.4 Implementing disposal of records
4.1.4.1 Destruction of records
Records sentenced for destruction must be destroyed in accordance with internal policy covering disposal of confidential material. Where records are due to be destroyed, backup copies stored on alternative media (server / microfilm / paper / CDs etc) should also be destroyed. This is vital to ensure compliance with the requirements of Data Protection and Freedom of Information legislation. For this reason it is essential that the master file or record, and the master format, be unambiguously identified at all times.

Transitory records may be destroyed routinely under standard operating procedures; however, they too must be destroyed properly and permanently in accordance with internal policy, and may be subject to litigation holds.

4.1.4.2 Litigation Holds
Litigation holds are outside the retention schedule but over-ride the retention period. If records are required, or are likely to be required, for litigation purposes, they should not be disposed of even if their destruction date has arrived.

“Likely to be required” means that there is a strong possibility of specific legal action, rather than that the records are the type of record used in litigation. Litigation does not need to have started, it is sufficient that there are indicators of litigation. If a litigation hold is placed on a file, then the file in question should be clearly identified as being subject to such a hold.

4.1.4.3 Long-term retention
As the records produced by the NHSBSA are public records they can not be retained for longer than 20 years without agreement by The National Archives (TNA). A retention period of this length, or longer, will only be applied to a very
small percentage of the information generated by the NHSBSA. Record types for permanent preservation will often include those of meetings of corporate leadership committees and groups.

Records identified in the schedule as ‘permanent’ are marked ‘Offer to Archivist’. The Archivist may choose to select a sample of the records for permanent preservation in the archives; the remainder should be destroyed as specified in the Guidelines. The sample may be random, selective or purposeful.

‘Offer to Archivist for review’ is used to indicate record classes where the Archivist will not usually be interested in retaining the class of records, but may wish to retain those concerning high-profile or controversial policies / projects.

Records no longer required for administrative use may still retain sensitive information. The Archivist should be informed of sensitivity at the time of transfer of the material to the archives, and an appropriate closure period agreed. The closure period should comply with Freedom of Information legislation and the NHSBSA’s policy.

4.1.4.4 Closure period

A specified period of time during which the record is subject to restrictions on provision of access to staff and/or the public may be dictated by statutory requirements or by the NHSBSA’s policy. This usually refers to the record after it has been closed to active use or has been transferred to an archival body. Length of closure period varies depending on the reason for closure, e.g., personal records transferred to archival bodies are sometimes closed for 100 years after the date of birth, 70 years after the date of death, or (where the information is very sensitive) 100 years after the death of the last member of the subject’s immediate family.

Further information can be found in the NHS Records Management Code of Practice (Part 2), on which the NHSBSA’s retention schedule is based for the most part. Another important source and reference model is JISC InfoNet’s Higher Education Business Classification Scheme and Records Retention Schedule.
5 An Introduction to the Business Classification Scheme (BCS) and File-Plan

5.1 Business Classification Scheme (BCS)
The Business Classification Scheme is a conceptual representation of the NHSBSA’s business. It describes business functions and activities, and the relationships between them. Functions represent the highest level of business activity – they are the major responsibilities that are managed by an organisation to fulfil its mission or mandate, and its responsibilities to its stakeholders. Activities are the sub-functions or tasks performed to accomplish each function.

While there are many ways of structuring a classification scheme – e.g. by organisational structure, or by location – the NHSBSA BCS follows best practice in categorising records by business function. A functional approach focuses on managing records according to their business context (why they exist) rather than their content or their location. Records management activities are thus linked clearly and firmly to business functions and activities.

The basic components of any functional BCS are:

- a hierarchical classification structure, with the top level containing the broadest categories of activity (i.e. functions) and the lower levels becoming increasingly specific (i.e. activities and their component parts);
- scope notes which define the scope of the categories.

The BCS may depart from a purely functional schema at its third or lower hierarchical levels, for reasons of convenience or logic. Thus, a patient is clearly neither a function nor an activity of a hospital, but it obviously makes sense to hold patient records in the form of case files in each patient's name rather than in series based on the different activities that take place around the patient's treatment.

5.2 File-plan
The BCS 'sits above' corporate and local File-plans, which are the embodiment of the classification scheme. The BCS and File-plan are not, however, identical: while the higher levels of a file-plan will generally coincide with its governing BCS, it will inevitably depart from a functional approach in the levels below the BCS, where the actual files and records are located. Files will be based on date ranges, topics, individual or group names, geographical location, etc.

At its lowest level, the file-plan will almost always contain a folder based on date, as one of its principal functions is to manage retention. To assign a retention period to a record, it must consist of or be contained in a folder to which a single date can be assigned.

File-plans are derived from pre-digital methods of recordkeeping and records management, where records were overwhelmingly held in paper folders, registers, etc. Unstructured digital records can be represented in much the same way – the folder view of files on individual C-drives or on shared network drives are file-plans, though without the application of corporate records management practice, they are organised according to individual preference rather than consistent principles.

Structured records, such as those held in line-of-business systems, are not easily assimilated to the BCS or file-plan, but should nonetheless be represented: an empty
folder called, e.g., ‘XYZ System Data’ could be inserted at the relevant node, to show that these records exist and to indicate their place in the overall scheme.

The file-plan should also incorporate the corporate Security Classification Scheme (see Section 6.3.2, 6.3.3) by noting restricted files or file groups. Just as the date information attached to folders in the file-plan act as a trigger for disposal under the terms of the Retention Schedule, so any security classification information can act as a trigger for making sure that the appropriate levels of security are applied to the relevant files.

5.2.1 Model File-plan

A fully articulated file-plan cannot be produced without a thorough audit or survey of the records held by each business area, which would reveal the actual records series in existence, the organising principles currently applied to them, and their relation to other series. In the meantime, model file-plans have been drawn up for a handful of the more generic functions (e.g. administering corporate committees, developing policy, line-managing staff). These are incorporated in the BCS.

The models provided are intended for guidance rather than to be followed rigidly; for example, the plans will mostly reflect a function / activity hierarchy, but if the system in use is case-file based, the folder hierarchy can be structured to facilitate this.

Two essential features must, however, be present:

(i) Retention decisions should be applied at the level of folders rather than documents, i.e. a folder should not contain documents with different retention periods.

(ii)Structures and conventions should be consistent and coherent – this applies especially in respect of those functions and activities (e.g. developing policy and strategy; certain HR and finance activities) that apply to more than one business area, where the file-plan should be identical or very similar across the BSA.

It is also highly desirable that the file-plan is logically and clearly presented to enable browsing and retrieval of files and documents – does it pass the ‘Temp Test’, allowing someone not already familiar with the business processes and the file subject-matter to reasonably deduce where a given file might be if they are asked to find it?

5.2.1.1 Assigning retention details to folders

In the models, the retention period has been assigned to folders by appending the date of disposal with the prefix ‘dis’ for disposal. This denotes the date on which the disposal action (e.g. destroy / review / send to archives) should be taken. Because the retention period starts when a record is complete or ceases to be active, rather than when it is begun, this information must generally be added at a later stage than that at which the folder is created. For example, the agenda for a meeting might be circulated well in advance of the meeting, but the retention ‘clock’ starts ticking when the policy is issued. In the examples given, the disposal date is generally given as the exact date plus retention period, but it will often be impracticable to apply retention decisions continuously; once it has been agreed and noted as a standard procedure, it would be possible to apply the retention schedule annually or at six-monthly intervals, even if that does mean that records created near the beginning
of a year might be held for quite some months longer than the retention period assigned to them.

More or fewer file / folder levels than those indicated in the model may be needed. For instance, in the sections of the file-plan relating to meetings of groups and committees, a folder level indicating the year has been included, with each meeting held throughout the year assigned its own sub-folder within that. However, if the group is short-lived or constituted ad hoc, it will probably not be necessary to include this level, but just have the folders for each meeting.

5.2.1.2 Reference material

Reference material: this is generally used for a specific purpose, e.g. drafting a document, and is classified as a transitory record, subject to the standard 3-month retention period for such records. The retention period ‘While being used’ is another way of expressing this.

Occasionally, reference material may be assigned a longer retention period depending on its purpose. If reference material – external publications, for instance – is of more general use, apart from the specific use it may be put to from time to time, it is advisable to set up a central repository in the form of a folder or folders specifically for reference documents so that the material is not subject to the transitory retention period.

Where the ‘master’ version of reference material is held elsewhere – e.g. an existing BSA record, or a document held in a ‘repository’ folder – it should be represented by a shortcut in the business file rather than a copy.
6 Requirements and Guidelines for Recordkeeping in the NHSBSA

*Records Management* is an agreed set of policies and procedures by which an organisation, such as the NHSBSA, takes corporate responsibility for its corporate information. *Recordkeeping* comprises the sets of procedures through which the NHSBSA practises good records management on a day-to-day level. Recordkeeping concentrates on activities at file and document level, and requirements can be adapted to suit local needs, though in keeping with corporate-wide records management aims and intentions.

Many of the business activities within the NHSBSA are managed within a structured environment (e.g., a business application) and in such an environment, creation and management of the necessary records may be forced. However, in some instances the required record may be a hybrid of information in a database and unstructured information (e.g., procedural information entered into a spreadsheet, and letters in a correspondence folder). Some processes are entirely unstructured. In both of the latter cases, intervention by those creating and maintaining the record is required to ensure that it is complete, adequate and appropriately managed.

### 6.1 Creating a Record

#### 6.1.1 When to create a record

Anything that is written or typed (or recorded) is potentially a record, so you should always be careful about what you commit to any kind of permanent form. The NHSBSA’s *Business Rules on Records Management* contains further detail on when and how records are to be created.

Records are created in forms and environments that can be either *structured* or *unstructured / semi-structured*:

**Structured records** are those created within, and that exist mainly as data within, business and database systems. The most familiar general examples include HR systems and payroll systems, ordering and purchase systems (e.g., Amazon), booking systems, etc. Even where the data itself is not limited to certain values, it is contained in a known field and exists in a known relation to other records and components of records within the system.

**Unstructured records** are those created in looser ways, primarily for processing by people rather than machines. They include documents, e-mail, images, audio or video recordings, photocopies, microfilm, etc., and may be digital or non-digital in form. In fact, this type of information is almost all *semi-structured*, since it generally has some structural elements – formal, such as a title or a salutation in a letter, or integral, such as the header information in an e-mail – but it is generally described as ‘unstructured’.

Most of the NHSBSA’s business streams are managed within a structured environment (i.e., an application which manages the progress of a particular piece of work such as payments to health professionals or investigations of fraud). Such structured environments will generally force the generation of records.

Within unstructured environments, there are some general rules of thumb about when you should consciously make an effort to make sure that information is recorded. Bear in mind that it is a good idea to tailor the kind of record to the
significance of the action. For example, there should always be a record of any meeting held. If this is a meeting of the Board, the record will be more formal or more extensive than a team meeting or a hand-over meeting, where the record might simply be an e-mail confirming the discussion.

The following are examples of business activities that should give rise to records:

- decision-taking, e.g., minutes of meetings, informal or formal agreements related to business activity, change control procedures
- changes in or review of policy, strategy or procedure
- changes in activity – e.g., producing new, or changing existing, policy or procedure, amendments to manuals or other procedural guidance
- engagement with governance – audit, procedure or activity reviews, any transaction (e.g., financial, health and safety, related to personnel) that may be subject to audit
- projects – even those that are either abandoned or deferred.
- transactions with internal and external customers, e.g., responding to enquiries, corporate communications (e.g., business information on intranet, press releases).

### 6.1.2 Naming conventions for files and documents

In some instances, data and documents created within a structured environment (e.g., within a database or a business-specific software application) have a certain naming convention built in. It is thus important, whenever any new databases or software are introduced, to assess the way in which it will automatically assign or force naming conventions in comparison to the NHSBSA’s requirements for naming.

Where records are generated in an unstructured environment (e.g., in Word documents or Excel spreadsheets), care must be taken to ensure that the title of the documents and the files in which they are stored are named in a clear, logical and sensible way.

Sometimes it will be easy to decide on a title for a file, e.g., where the business process is based on cases (applications, investigations) the title will most usefully be the name of the individual or (if appropriate, e.g., during recruitment) a unique reference number. It may help to consider the file path as the entire file name, and judge whether or not all of the elements of the file path create a file name that will make very clear what the document is about and why it is stored where it is.

In addition it may help to remember to avoid personal names and ambiguous phrases like "stuff", "miscellaneous" or acronyms that will not be familiar to everyone. Also avoid using subject headings as file names: “Consultation 2008” does not clarify whether BSA was conducting a consultation, responding to one, or whether this file is just a reference copy of someone else’s work. It is easier to apply Retention Schedule requirements when the context of the file or document is clear and unambiguous, and it also helps ensure that the Schedule, the Business Classification Scheme, and the Corporate File-plan are accurately maintained.

Remember that the naming conventions apply regardless of where the record or file is stored, that is, the same rules apply whether the document is in a hard-copy file, an electronic file or stored in an e-mail folder. Every filing system should use the same names; this is similar to the requirement that all parallel filing systems are structured in the same way and according to the corporate file plan.
6.1.2.1 *Use the corporate file-plan to structure your files*

Use the corporate file-plan to structure your files, and use the terms provided.

The top-level (Function, Activity) folders should generally contain full rather than abbreviated terms, and should always retain the verb-form for the 'action' element in full. Thus, although it may be legitimate to have an agreed abbreviation 'Project Mgmt' as a folder heading lower down the order, if managing projects is a Function or Activity at the higher levels, the folder should be named 'Managing Projects'. This keeps the emphasis on the purpose of the Business Classification Scheme, which is to describe the business actions of the BSA.

6.1.2.1.1 *Structure files to support the Retention Schedule*

The volume of records generated by any organisation means that it is almost never possible to manage retention periods at the level of the individual document or record. For this reason, it is important to organise records, whether digital or non-digital, in file and folder structures that support the implementation of the Retention Schedule. This enables disposal to be carried out at the level of groups or batches of records rather than at the level of the individual record.

The most obvious examples of this within the NHSBSA are high-volume batched records, such as prescription forms, or financial records which are held in batches by year or year and month. But the principle applies to other records too. For example, one of the activities of line-managing staff is managing annual leave; substantive records of each year's leave are scheduled to be kept for two years. It is therefore not enough to have all of an individual's annual leave records held in a single file called 'Bloggs J', or even to separate them out in a folder called 'Bloggs J Leave' – there will need to be sub-divisions for each year, so that each year's leave records can be disposed of in turn when two years have passed. Or, using a different structure, disposal actions might be applied to a folder called ‘2009 Annual Leave’ and all of its sub-folders ‘Bloggs J’, ‘Other A N’, etc.

In digital files on a networked drive, this can be achieved by having sufficient levels of subfolders. A similar approach applies to paper files, except that where the number of documents is low, it is sufficient to create virtual 'sub-folders' by using internal dividers in a single physical folder to separate out the records to which the same disposal date applies – what matters is that the relevant records can be easily identified as a group rather than by having to search through the whole file.

6.1.2.2 *File names should be short, but meaningful*

This is greatly facilitated by including a verb in the title, so the activity being recorded is quite clear. “Training” is insufficient as a file title – is this training received, being planned, being delivered or being arranged? The exception to the use of a verb to assist clarity is where the file contains reference information only, rather than working documents. In this instance the file title could be “External Reference – Training”.

6.1.2.3 *Avoid repetition when naming sub-folders*

Avoid the addition of redundant folder levels – new levels should always follow a logical or, occasionally, a purely practical necessity.
Allow for inheritance of metadata / information from higher-level folders: e.g., if there is a folder named 'BSA Committees' and a subfolder called 'BSA Committees – Meetings', the latter should be changed simply to 'Meetings'. The file-path makes it clear that these are meetings of the BSA Committees.

**Note:** This applies to folders only; at the document level, inheritance cannot be assumed since documents are frequently detached from their context, e.g. when sent as an e-mail attachment.

(As the file-path is an important contextual metadata element, it should be incorporated in the visible metadata of each document created, in the header / footer or elsewhere.)

**6.1.2.4 Avoid using non-alphanumeric characters in file titles**

Avoid using underscores or hyphens to delimit words in a file title, where possible, and use capital letters instead. This avoids both unnecessarily lengthening the file name and running the risk that other users’ computers and systems may not recognise such characters.

**6.1.2.5 Add the date of creation to the file title**

The date on which a file was created (or received, where possible) should be included in the title, in the form YYMMDD. Thus, a letter or e-mail sent on 24th January 2010 should be titled something like ‘Stationery Request 100124’.

If the date is used as an organising principle for the record or record series, put it first and in the form YYYYMMDD, as outlined in 6.1.2.6 next.

**6.1.2.6 If the date or identifier is part of the file or record title, always make it the first part of the file name**

Where a record includes a date as part of its name use the format YYYYMMDD (or YYYYMM or YYYY, depending on the level of detail required). This will mean the records will automatically be ordered chronologically and therefore easier to manage.

Similarly, and for the same reason, if a numeric or alphabetic identifier is part of the file or record name, make it the first element of the name, and make it at least a 2 digit number (i.e., 01, not 1).

One example of such files and records would be, e.g., financial transactions filed year by year, where a folder might be called ‘2009’ and the files within it ‘20090103 Payment for x’, ‘20090215 Payment for y’. Another would be a series of case files using an individual’s name as identifier: the files should be titled, e.g., ‘Smith John A’ rather than ‘John A Smith’.

**6.1.2.7 The version number of a record should, where applicable, be included**

It is essential to identify different versions of records to avoid using or sharing out-of-date records.

Distinction should be made between drafting versions and stable, released versions: drafts should be assigned version numbers of the form v1.01, v1.02, etc while final versions have only zero behind the decimal point, e.g. v3.0.

The ‘final’ draft version should be saved as e.g. Doc Name Draft v1.06=Final v2.0 with Track Changes intact, and a separate copy saved as the actual final version.
with all changes approved – this keeps an audit trail of the amendments while allowing the production of a 'clean' final version. Where records are subject to periodic update, this process is iterative, as in the example below.

Example: Business Continuity Strategy Draft v0.01 081213
Business Continuity Strategy Draft v0.02 090109–Final v1.0
Business Continuity Strategy v1.0 090124
Business Continuity Strategy Draft v1.01 100203
Business Continuity Strategy Draft v1.02 100210–Final v2.0
Business Continuity Strategy v2.0 100227

6.1.2.8 Use only agreed abbreviations
Avoid using abbreviations unless they are very standard, or are very well known across the organisation. Even then, there should be agreed forms to prevent, e.g., one person using ‘NHS’ and another, ‘N.H.S.’

Idiosyncratic abbreviation will make it more difficult to find files. If, for instance, 'Information Governance' is always found either in its full spelling or in the abbreviated term 'IG', then only two search terms at most are required; however, if there are ‘privatised’ variants such as 'Info Gov', 'Inf Gvnce', etc, there can be no confidence that even multiple searches will find all of the required files.

6.2 Filing and Locating Records
Records should be filed and stored systematically, in line with the Corporate File-plan and any local file-plans, and following any Standard Operating Procedures and guidance. This is particularly important when dealing with unstructured records and recordkeeping environments, since there are few if any system constraints to ensure good practice: poor filing greatly diminishes the NHSBSA’s ability to gain access to and retrieve its records in a timely fashion, and may result in the permanent loss of important information.

6.2.1 The role of guidance and Standard Operating Procedures (SOPs)
Local rules and SOPs should include instructions on where to file records and documents, electronically and in hard-copy; how to identify them; how to classify them (if this is not an automatic procedure); and how to apply Retention Schedule requirements.

Induction procedures for new staff should include instructions on how and where to save their records; staff who have Personal Assistants or the equivalent should be required to provide all of their records to the assistants to file, rather than doing so themselves.

Records and files include e-mails, so staff must be clear about who is responsible for retaining an e-mail, whether the sender or the recipient (generally the sender). Consider including a reminder to this effect (if it is a standard rule) in the footer of internal e-mails. In some instances, guidance for staff should include assignment of responsibility for creation of records, e.g., in rules for setting up groups / committees, assign responsibility for creating minutes.

6.2.2 Filing a record on creation
When creating a record in an unstructured environment, determine whether there is a file already in existence to which the record belongs; if not, open a new file.

• Identify where in the file-plan the record should go.
• If you are not sure about this, contact your local records manager for advice.
• Give the file a name that describes the activity being recorded; use the naming conventions in Section 6.1.2 above.

6.2.3 Electronic Files vs Paper Files
It will not usually be necessary to maintain a hard-copy and an electronic system simultaneously, though it may occasionally be necessary to have a hybrid file (i.e., one containing both digital and non-digital records). The difference is that there is rarely any need to have hard-copy of material that is stored electronically, though there may be occasions when a predominantly electronic file has a hard-copy element.

• Where one file is maintained in more than one format each format should be filed and titled in exactly the same way.
• The existence of the hard-copy element can be indicated either by including as an entry on the electronic file-plan or by creating a “dummy entry” in the electronic folder, which has the document title “Hard Copy Element”
• The same retention period applies to a file in all its formats, and also to any duplicates.

6.2.4 Retrieving records
Staff should not rely on the “search and retrieve” facility of computer systems to successfully locate records. Unless a search is extremely focussed (which is usually only the case within specific applications) and is being performed on records series containing a high level of accurate metadata, searches routinely bring back an insufficient response, or far too many records, which then have to be assessed for relevance. Filing and location of electronic records is as important as it is for physical records.

A good rule of thumb for assessing whether or not filing practices and decisions are of good quality is “the temp test”, also known as “what happens if you win the Lottery.” If the filing system is explained to a reasonably proficient temporary member of staff (the point being that they will not be familiar with usual practices), will the temp be able to use it? If a member of staff radically changes their lifestyle at short notice, and someone else has to take over their work, will they easily be able to identify and locate the records needed to show what work was being done, how and why? If yes, then the filing system works. If not, then it needs attention.

6.3 Records and Information Security
Records and other information are created or held by the NHSBSA to enable it to carry out its various business functions and activities. It follows from this that most of this information is sufficiently important that its loss or misuse could have a serious, even critical, negative impact on the NHSBSA’s capacity, authority, and credibility.

In general, information security addresses two aspects of information – value and confidentiality. Information is an asset and, like any thing of value, may need to be protected from loss or misappropriation. It is also a powerful possession, access to which may need to be restricted for legitimate reasons of safety, privacy, commercial advantage, public interest, etc.

This section deals primarily with preserving the value and confidentiality of records through restrictions and controls on access and transfer; the preservation of records
and other information for business continuity purposes is covered in Section 8 on Business Continuity and Preservation.

6.3.1 Basic records security

There are a number of fundamental practices that help maintain the security of the records and information for which the NHSBSA is responsible. These practices apply to all records and information, but the potential repercussions of failing to carry them out are greatly amplified where the records are vital or valuable to the organisation’s business, or contain confidential material.

Further information can be found in the Information Governance, Information Security and Data Handling and Storage policies, and in the Data Classification Matrix, but some essential points are:

- never transfer digital information outside the NHSBSA unless it has been encrypted or sent through a secure channel
- ensure that physical files and media are sent using a delivery method appropriate to their level of value or confidentiality
- never save or copy corporate records and information (i.e., any work-related documents, e-mails, etc) outside the networked environment (e.g., onto PC hard drives or removable media such as CDs or flash drives), except as a temporary measure to facilitate off-line or off-site working; in such cases, always delete the copy after use
- never leave physical or digital files and media unattended in unsecured areas, whether on or off site
- never share information in any form, written or oral, unless the person it is being shared with is entitled to have access to the material.

6.3.2 Security classification – All NHSBSA directorates apart from CFSMS

NHSBSA creates, holds and uses a lot of information that is confidential or sensitive. In areas of activity such as personnel, finance, procurement and investigations, the greater part of the information created and received will be confidential or sensitive.

In addition to this, there are activities where the bulk of the record is non-confidential, but where there is some sensitive information. Examples will include processes for responding to requests for information, where most of the record is open but may contain personal data, such as name and contact details.

In some cases, the fact that records are confidential will be very clear and unambiguous, and may be part of the business process, or the record itself (e.g., contracts which will state their confidential status). If it is unclear whether a record or a file is confidential or not, it may help to think about what the consequences would be if the record or file were made public.

The nature of the work undertaken by the Counter Fraud and Security Management Service (CFSMS) necessitates a more rigorous approach to information security than is required for the type of information created and used in the rest of the NHSBSA. CFSMS therefore uses the Government Protective Marking Scheme to classify and protect its information assets. The separate requirements of this scheme will be dealt with in Section 6.3.3.

---

12 NHSBSAIMG002 NHS Business Services Authority Information Governance Policy
13 NHSBSAIS001 NHS Business Services Authority Information Security Policy
14 NHSBSARM017 NHS Business Services Authority Data Handling and Storage Policy
The Data Handling and Storage Policy lists the security classifications in use in the NHSBSA, and the Data Classification Matrix\textsuperscript{15} sets out the appropriate methods of treating public, internal, confidential, and restricted information held in various formats. Local file-plans should incorporate the matrix by assigning the appropriate handling classification to each file or record series. Any security classification scheme will cover the following generic categories.

6.3.2.1 Low Confidentiality Level
The information has been authorised for publication or public access, and could be disclosed without any redaction at all. Examples include:

- information that is designated as accessible on demand within the NHSBSA’s Publication Scheme (e.g., finalised policy documents, certain organisational information).
- published material – reports, information booklets or leaflets, etc.
- anonymised or statistical data
- minutes of Board meetings, once the minutes have been approved and redacted to remove any information that is exempt from disclosure.

6.3.2.2 Medium Confidentiality Level
The information could be disclosed but only after some alteration (e.g., removing personal names), or may be subject to a temporary embargo on disclosure (e.g., it could be disclosed once an appointment was made, or a policy confirmed). In the latter case, the record will be confidential for a specified period of time, but when it comes to disposal, it will no longer be confidential.

At times, the alteration will be sufficient to allow the record to be made public; at others, it will merely enable it to be disseminated more widely within the NHSBSA.

Before any such alteration, the records / information must not be disclosed to any person who does not have a legitimate need to access the information in the course of their work for the NHSBSA. Such information includes:

- information (other than personal data) that must not be disclosed without the permission of the data owner
- personal data that must not be disclosed to third parties unless
  - the consent of the person who is the subject of the data has been obtained; or
  - Some other condition(s) set out in the Data Protection Act 1998 has been met.
- committee or working papers on matters of current business that are not yet intended for wider dissemination or consultation.

6.3.2.3 High Confidentiality Level
This level applies to privileged or proprietary information that could cause significant harm (including operational financial, legal or reputational damage) to the NHSBSA or to individual(s) if compromised through alteration, corruption, loss, misuse, or unauthorised disclosure. Sometimes, such information cannot be disclosed to the public or more widely disseminated within the organisation at all; at other times, this may be permissible but only when one or more conditions had

\textsuperscript{15} http://www.nhsbsa.nhs.uk/Documents/NHSBSACorporatePoliciesandProcedures/Data_Classification_Matrix.pdf
been satisfied. Highly confidential information might be fall into one of the following categories:

- the record cannot be released at all and restrictions on access must remain in place throughout its existence
- the record cannot be released without considerable removal of restricted information (e.g., personal, medical or complaints files on identifiable individuals)
- the record cannot be released while the information it contains remains current and its wider dissemination could impede the legitimate activities of the NHSBSA (commercially sensitive information, information related to current legal cases).

6.3.2.3.1 Personal Data
Highly confidential personal data is information that would cause significant damage or distress to an individual if disclosed or shared without their consent. Examples include:

- sensitive personal information (as defined in Section 2 of the Data Protection Act 1998)
- information such as personal bank account and other financial information and national identifiers, such as national insurance numbers and copies of passports and visas
- personal information relating to vulnerable adults and children
- detailed information on staff, such as work performance, salaries (unless subject to statutory disclosure), personal life, sensitive negotiations, or information that would compromise their safety and security.

6.3.2.3.2 Other Data
Access to certain records and information needs to be restricted as it could have negative effects on the NHSBSA’s ability to work effectively or meet its legal and other obligations, or because it would be damaging to the organisation, its staff, or its assets. Examples include:

- information received in confidence .e.g. legal advice, proprietary information received from contractors, suppliers and partners
- information that would substantially prejudice the commercial interests or competitive edge of the NHSBSA or its stakeholders and partners if disclosed
- information relating to high-profile strategy or policy development before the outcomes have been decided and announced
- information that would compromise the security of buildings, equipment or assets if disclosed.

6.3.3 Security Classification
The Government Protective Marking System (GPMS) requires that records and information be assigned labels – "protective markings" – that reflect the value and sensitivity of the record.

Five different markings are available; as with the classifications given in 6.3.2, the appropriate marking is dependent on the likely consequences of disclosure or unauthorised access:

- Official
• Secret
• Top Secret

Some records will not need to be marked, or can be marked ‘Not Protected’ – these correspond to the type of record with a low confidentiality level, covered in 6.3.2.1 above.

Disclosure of personal information is governed by the requirements of the DPA, as in Section 6.3.2, unless overriding factors such as criminal or legal investigations and proceedings require such information to be disclosed to appropriate authorities and agencies.

Full guidance for staff on applying the Protective Marking System should be sought in local procedures and documentation.

6.3.4 Managing access to records

Access to records can be facilitated or restricted in a number of ways. At the basic level, files and documents can be marked (physically or digitally) as ‘Official’. They may be locked away or password-protected. Access can be monitored by simple signing-in sheets. At the other extreme, dedicated secure facilities, state-of-the-art technology, and intensive screening and identification processes are deployed to protect the information and regulate access to it. No matter at which end of the spectrum an organisation is positioned, the principles are the same, and depend on good procedures properly observed and regularly updated.

The following paragraphs deal primarily with access to records that are restricted in some way, but this is not to say that there should be no control over access to unrestricted records. At the very least, physical records that are taken out for temporary use should always be signed for, and schedules and logs should always be kept of transfers of both non-digital and digital records outside the NHSBSA. Detailed procedures about tracking the location, use, and movement of records should be included in local rules and SOPs. Additional or different procedures may apply to CFSMS records that carry protective markings.

6.3.4.1 Restricting access to records and information

The function to which a record is related will usually indicate whether or not there is likely to be an access restriction. For example, if an activity is focussed around a tendering process or activities related to individual staff management, then it will be part of that process to restrict access to information.

Where a record is categorised as having a Medium or High Confidentiality level, robust procedures and controls must be put in place to identify the people who should have access to the material; to prevent unauthorised access; and to monitor access and use.

Always err on the side of caution.

Where entire processes are confidential or restricted then security can be placed at a distance, e.g., by having a secure server just for storing this information, or by setting security access codes or card-readers on the doors to the relevant work areas. If access is restricted intermittently in a process, this can be managed by protecting the documents in question, e.g., by requiring a password to open or update a document, or by putting files in a locked cabinet to which only certain staff have access. This may be the case where the restriction is time-limited (e.g.,
where commercial sensitivity only lasts until a contract is awarded) or until the sensitive information is removed (e.g., by weeding out personal information).

The fact that files or records have restrictions should be noted on the local file plan, as it may affect retention periods (e.g., a file holding personal or sensitive personal information may need to be weeded whereas other files in that series may not). Records that contain personal information about living, identifiable people have to be handled carefully, even if the rest of the file contains unrestricted material.

6.3.4.1.1 Records containing both restricted and unrestricted material
Many files will contain information at different levels of confidentiality; this has been alluded to already in describing the possible need to ‘weed’ files of confidential material to allow their wider dissemination.

There are a two possible ways of dealing with the confidentiality categorisation of files that contain confidential material: (a) the confidential or sensitive information can be removed and held separately in an associated file, so that the main file can be treated as unrestricted, or (b) the confidential material can be left in place and the entire file categorised as confidential.

A business area may make its own decision, based for instance on cost and efficiency, as to which of these approaches to take, once this does not contravene statutory or binding requirements on the publication of information and records. However, any saving in cost or gain in convenience must be offset against the NHSBSA’s declared commitments to transparency and openness and to good information governance.

Ideally, all information that can be shared or published should be. If in doubt, contact the Records Manager or the Information Governance section.

6.3.4.2 Tracking the location and use of records
Access to electronic files can be automatically audited. However, if a hard-copy parallel system is being maintained then these files must also be kept secure and should also be tracked. Where the volume of records and/or usage is low, then this can be done manually, e.g., by having a borrowing docket or form on the front of the file. However, where the volume or usage is high, then it may be necessary to consider electronic means of control, e.g., bar-coding or use of RFID-tags.
6.4 Disposing of Records

When records cease to be of use to an organisation, or when there are legal requirements concerning the length of time for which or the places where they may be kept, they must be disposed of. ‘Disposal’ does not necessarily mean ‘destruction’, though that is one means of disposal. It can also mean transfer to another location, custodian, or format – for instance, certain records may be sent after X years to a corporate or external archives, or records in certain formats may have to be migrated to new media every Y years.

**n.b.** It is important to remember that if a record is due for disposal, all copies must be disposed of, including those contained on removable media (e.g., CDs). Occasionally, this may mean that a copy can be legitimately kept (e.g., to keep on-site copies of records sent to The National Archives under the Public Records Act), but in the vast majority of cases, it means that all copies must be destroyed (this is obviously the case where the record is scheduled for destruction).

Instructions for the disposition of records and record series is found in the NHSBSA’s Corporate Retention Schedule (see Section 4). Each business area will have a local retention schedule derived from the Corporate Retention Schedule.

6.4.1 Litigation holds

If records are required, or are likely to be required, for litigation purposes, they should not be disposed of even if their destruction date has arrived. Instead, a ‘litigation hold’ is applied, which means that the records must be held until the case has been resolved.

“Likely to be required” means that there is a strong possibility of specific legal action, rather than that the records are the type of record used in litigation. Litigation does not need to have started, it is sufficient that there are indicators of litigation. If a litigation hold is placed on a file, then the file in question should be clearly identified as being subject to such a hold.

6.4.2 Documenting the disposal of records

The NHSBSA must be able to account for all of the records and information that it creates and uses; this responsibility does not cease when the time comes to dispose of the record.

Every file – or in certain high-volume record series, every volume or batch – that is transferred or destroyed must be documented on a transfer or destruction list, which should be signed off by an appropriate person. This is essential for audit purposes and to prove, if required, both that the information is no longer held by the NHSBSA and that it has been disposed of in accordance with records management policy and procedures rather than arbitrarily or irregularly.

Because different storage facilities and file tracking systems may operate or be configured in different ways, transfer and destruction schedules will need to accommodate the requirements of each facility and system to provide all the information needed to identify and manage disposal. These requirements should be laid out clearly in local rules and SOPs.

For using a records register as the basis for transfer schedules and disposal lists, see 6.4.2.2.1 below.
6.4.2.1 Structured record environments

For digital records, it will generally be possible to generate system reports to provide at least the backbone of the list. In structured records environments within the BSA (e.g., where business activities are managed within a software application), retention, disposal and holding functions can be performed via the application. Records can be identified as requiring deletion or files can be flagged as being on hold. The software application will usually also maintain a list of the files which have been deleted, which is a requirement where records are public records; at the very least, it ought to be possible to run a query on the system and output a report prior to deletion. In an unstructured environment, this process takes more active management, though it is possible to export the file structure of a shared drive as an XML or CSV file prior to permanent deletion.

6.4.2.2 Unstructured record environments

Outside of an electronically structured environment there is no automatic or single-step way to actively manage records. For non-digital records, any list will involve some level of manual input, though this can be minimised through the use of technology.

6.4.2.2.1 Maintaining a records register

The simplest way to manage the retention, disposal or holding of unstructured records is to maintain a file register. This is a list of all the files that are held in relation to a particular business function. The local copy of the file-plan can be used as the local records register. It requires an extra step when a file is being opened (i.e., the file name and opening date is added to the register) but no extra work when saving a record.

The files may therefore be held by an individual member of staff or by several members of staff, each with responsibility for different records. Regardless of which is applicable there should be only one register. The register can then be used to help when looking for information, particularly where a type of information is being sought, or when checking whether or not we hold information, where the “search and retrieve” facility on the computer is less useful.

It is useful for planning to weed or destroy files, as the age of the file from the day it was closed is usually a trigger for reviewing unstructured files.

It can also be used as a basis for a transfer schedule (if files are being sent to off-site storage or are being transferred to The National Archives), and copied and retained as a register of files which have been destroyed. This is important for audit purposes, it is a requirement where records are public records and is also useful in the case of queries about information governance (e.g., if an FOI request is made and the organisation wishes to demonstrate that the file was sent for destruction before the request was received or processed and not afterwards).

The register can be used to manage litigation holds. This can be a fairly simple device, such as using an agreed colour in the cell background, or an agreed colour for the text of a held file. If the register is used to manage holds, then it will need to be adapted so that it can also record the date on which the litigation hold was requested, the name and job title of the person making the request, and the end date if it is known.
The register should also indicate whether the file is in hard-copy or in electronic format. The majority of master records will be (or should be) electronic. There is almost never a justification or requirement for maintaining both a hard-copy and an electronic filing system. Where it is necessary to maintain a hard-copy and an electronic copy filing system, they should have the same names, contain exactly the same information and should be weeded and disposed of at the same time.

6.4.3 Destruction of records

The majority of records can be destroyed in a straightforward manner, by shredding or recycling, though if the record is sensitive (e.g., it contains personal information) then it will need to be securely disposed of in accordance with HSCIC guidance available at


It is important to remember that simply ‘deleting’ a digital file from a server or hard drive does not destroy it: the record must be destroyed beyond any possibility of reconstruction. This applies whether or not the record is scheduled for secure destruction. Remember that most modern scanners, photocopiers, fax machines etc store cached copies of the documents they process – these cached copies should be purged regularly.

Records sentenced for destruction must be destroyed in accordance with internal policy covering disposal of confidential material. Where records are due to be destroyed, backup copies stored on alternative media (server / microfilm / paper / CDs etc) should also be destroyed. This is vital to ensure compliance with the requirements of Data Protection and Freedom of Information legislation. For this reason it is essential that the master file or record, and the master format, be unambiguously identified at all times.

Transitory records may be destroyed routinely under standard operating procedures; however, they too must be destroyed properly and permanently in accordance with internal policy, and may be subject to litigation holds.

6.4.3.1 Confidential records

Confidential paper files can be shredded, incinerated or pulped, depending on what is most convenient for the business area. However, regardless of which of these three options is chosen, each business area must have:

- a form of certification
- a clear process that differentiates between confidential and unrestricted.

Many commercial disposal facilities will provide certification of confidential destruction, and each business area will need to have a person (e.g., the Local Records Manager) designated to ensure the certificates are received, that they are kept together, and that it is clear to which destroyed batch the certificate relates.

Most areas of NHSBSA have recycling procedures, but while these may be used for unrestricted records, it must be physically obvious where are the confidential records and where the unrestricted. The most usual way to do this is to have the paper collected in differently coloured bags, e.g., red for confidential. Avoid using green or black for confidential waste.
If the amount of confidential waste requiring destruction is very low, and it is more economical for staff to spend the time shredding the files:

- get as large a shredder as is possible – otherwise the process will be so slow that it will be difficult to find time to do it, staff will be more likely to be interrupted and leave the work unfinished, and the machine is more likely to jam
- make sure that the shredder meets the standard requirement for fineness of shredding, or that it cross-shreds. This is necessary for highly confidential material.
- provide a mechanism for certification – this may be an e-mail of confirmation from the person responsible for shredding to the Local Records Manager, identifying the confidential records shredded, and an acknowledgement in return. Whatever process is decided upon it must be consistent, and the certifying process must be recorded. The Local RM should be able to show where all such certification records are kept, and demonstrate to what records they relate.

6.5 Managing changes in staff or the recordkeeping environment

6.5.1 Staff – starters and leavers

6.5.1.1 New staff

The main responsibility of managers and local records managers when a new member of staff joins the NHSBSA is to ensure that all the relevant information about corporate and local records management requirements is successfully imparted. There is an on-line training programme which all new members of staff must complete within their probationary period, and there are corporate records management guidelines and policies available on the intranet or on request. In addition, local operating procedures or manuals should cover how records are created, managed and disposed of locally, including guidance on storage and security markings.

6.5.1.2 Leavers

It is particularly important to be clear about what happens when an individual is leaving the NHSBSA. The main focus is to ensure that there are no unclear or unsorted records left which will be inherited by their colleagues or replacement, since it is rarely possible for a new member of staff to be in a position to make decisions about records whose context is unclear and which the new staff member did not create. All too often, such records to simply hang about in limbo, with no clarity about their status or use. This is an additional reason for maintaining clear and accurate metadata, as staff who are about to leave an organisation will rarely have enough time to complete everything that they wish to complete, let alone re-write metadata.

The primary records and information responsibility for a member of staff who is leaving or who is moving to another area of the NHSBSA is that all relevant information is made available to their successor, all irrelevant information is disposed of appropriately, and that all personal information is deleted. Staff who are about to leave or move should ensure that:

- all of their live files are stored in a shared area or system, using the file-plan
- all of their semi-current files are listed and available, including any documentation detailing transfer to off-site storage
• lists of destroyed material are up-to-date and that any current litigation holds are recorded
• live files contain the most current versions of all their work
• all other hard-copy and electronic copies, including copies created for off-line or home working and copies on removable media, are destroyed
• at least one other member of staff has access to any passwords or encryption keys that are required
• e-mails reflect the file with which they are associated – live ones should be in live files (and e-mail filing structure reflects their electronic / hard-copy structure, so the relationship is obvious), semi-current in semi-current, and those for deletion should be deleted before leaving
• all personal e-mails, records, internet “personal favourites” links and voice-mails should be deleted
• the local records manager, and central Records Management, know that they are leaving.

6.5.1.2.1 Knowledge Management
It is also valuable to the organisation to be able to access at least some of the intangible, and often informal, knowledge that staff have built up over their time in post.

If you are about the leave the NHSBSA and are involved in on-going projects or tasks, you should create a resource for your successor so that they know where to find the information that they will need:
• create a Resources document for any informal or random information that you have built up over your time in post – for example, names and contact details of colleagues or external contacts who will be of value, any information about anomalies in systems or procedures
• create a reference resource of records or documents from other sources (either external or internal) which, though not directly related to a specific activity, may be informative. This can include internet sites links.

6.5.2 New business activities and processes
It is important that business areas notify the corporate Records Management area information about new activities. There are two reasons for this: to support corporate records management and to improve business practice. It may be necessary to adapt the records management documents (retention schedule, classification scheme and file-plan) to reflect the new activity. The new activity may involve new requirements for creating, processing or holding records, which need to be assessed for impact and which can be subsequently shared with any other business area which develops the same requirements.
7 Best practice for managing e-mail

e-Mail is an extremely useful tool, but its very popularity creates a range of problems. The general user frequently feels overwhelmed by ‘information overload’ and resorts to a fire-fighting rather than a planned approach to dealing with e-mail. At a corporate level, the informality and lack of rules generally found in the e-mail environment create significant, sometimes grave, difficulties and risks in relation to information governance and records and information management.

While the guidance given below cannot hope to cover all aspects of e-mail use and management, it is intended to give an idea of best practice at a reasonably specific level, and which is capable of extrapolation to similar cases.

7.1 General points on managing e-mail

1. Designate regular times to check for new e-mails – this is less distracting than always having it open.
2. Do, Delegate, Delete – try to take one of these actions with every e-mail; this will help keep the number of e-mails reduced.
3. Use the subject line as a document name – it should reflect what the e-mail is about – and where possible, its importance, e.g., “Informal”, “For Action”, etc.
4. If the message is short and simple (“Phone the Records Manager”) put it in the subject line and use EOM (end of message) to save colleagues’ time.
5. Weed your e-mails regularly and set your e-mail up to empty the Trash folder when you shut down the application.
6. Set your e-mail options so that it does not include the previous message in your reply. This helps prevent long e-mail strings that are very difficult to manage. (There may occasionally be exceptions to this, e.g. in cases where preservation of the string is specifically stipulated as an audit requirement.)

7.2 e-Mail and Records

E-Mail is often thought of as an informal communication medium, and e-mail messages as informal documents that do not have the status of records. This is not the case. If an e-mail relates to the conduct of the BSA’s internal or external business, it is every bit as much a record as a formally signed and sealed contract or deed. Because the informality of the medium gives rise to a huge ‘sprawl’ of e-mails, many relatively trivial mails that nonetheless are records must be managed in full compliance with the BSA’s records management policies and procedures.

Records can be divided into three broad classes. The contents of substantive records are essential to understanding and maintaining accountability for the business decisions and activities undertaken by the NHSBSA; an example could be a policy document, or the minutes of a meeting, or non-routine correspondence (received or sent).

Administrative records are not trivial, but relate more to the ways in which business activities are carried out rather than to their substantive activities and decisions – e.g., for a training course, the attendance sheet would be a substantive record, but the booking of trainers, rooms, AV equipment etc would be administrative.
Finally, **transitory records** are records of purely temporary or ephemeral value, which contribute towards the creation of other records but need not themselves be kept as part of those records. They include reference material, rough notes, and routine facilitative records. Fuller details are given at the end of this document.

Transitory records are still records, but can be deleted after their immediate usefulness has ceased – the period specified in the corporate Retention Schedule is 3 months after the activity they supported has been completed.

One of the principal approaches to managing e-mail as records is to ensure that insofar as possible, *e-mail is used only to create transitory records*. This means that, while still complying with the NHSBSA Business Rules and Standard Operating Procedures, as many mails as possible can be retained in the e-mail system and deleted after 3 months. e-Mails that constitute substantive (and, ideally, administrative) records should be saved out of the e-mail system into the appropriate recordkeeping environment, e.g. the corresponding file on a shared drive.

### 7.2.1 Additional points on managing e-mail

In addition to Points 1–6 above, which are part of good records and information management as well as contributing towards efficiency, the following practices and procedures should be adopted for corporate e-mail.

7. Avoid making comments or documenting decisions in e-mail – use the e-mail as the carrier or envelope, not the message. Some examples of how this can be done are:

- If a document is drafted and put out for comment, the comments should be made on a shared version of the actual document (either using ‘Track Changes’ or by inserting comments). Then if you want to notify the author that you have made your comments, just e-mail them to say that the comments have been added to the draft. This way, the record version of the comments is the document, not the e-mail.

- If asked to give comment or make a decision in general, and where it is necessary or most convenient to reply by e-mail, create a memo or letter (use templates for maximum efficiency) to record the decision etc, then send it as a link or (only if necessary) an attachment. Again, the e-mail becomes a transitory carrier of the ‘real’ record. This might seem a longer process, but is probably no longer than it would take to save all the relevant components of the e-mail out of the system and onto the core file afterwards.

If the use of e-mail as a format for substantive or administrative records is unavoidable for some reason, then the following points apply.

8. Avoid multiple subjects in an e-mail – if you want to speak of a new topic, where possible send a different e-mail.

- If an e-mail (like any other document or record) refers to more than one case or topic, a copy will generally have to be made and filed for each topic. This creates inefficiencies, but also creates difficulties relating to records retention and information governance – the different topics may be subject to different requirements for keeping and accessing them, for example
• Where you have no control – e.g. if responding to an external e-mail – make and file separate copies for each subject and respond to each with separate letters, memos, or e-mails.

9. Save substantive and administrative e-mails out of the e-mail system and into the same folder as other related records.
   • Where the subject of an incoming e-mail is blank or meaningless (e.g. ‘The finance stuff you were looking for’, a meaningful subject title should be appended if it is possible to do so without changing the original details.

10. If, for whatever reason, your unit or department does not conform to the practice of saving e-mails out of the e-mail system, the folder structure and file naming conventions must be the same as in your other electronic, and your hard-copy, systems.
   • e-Mails kept within the e-mail system must be managed in the same structures and to the same levels of compliance as records in shared drives or line-of-business systems. They are subject to the requirements set out in the Retention Schedule and to security and access requirements. Since these requirements are managed in part through the logic and structure of the Business Classification Scheme and file-plan, the folder structure in the e-mail system must duplicate that in the ‘main’ folders.

11. Never save e-mails to your PC’s hard drive or to external media, except as temporary off-line copies driven by a business need to work off-site or off-line. (This applies to all items, not just e-mail.)
   • e-Mail records are corporate documents, and must be managed in corporate recordkeeping and systems environments. Keeping records and information in systems or locations where they are not available for appropriate management and inspection both contravenes the NHSBSA’s requirements to comply with relevant legislation and best practice and compromises its ability to account for its business activities and / or gain access to its corporate assets.

7.2.2 Further note on transitory records

Transitory records include:
• routine material that facilitates day-to-day operations but does not set policy, establish guidelines or procedures, certify a transaction or become a receipt
• documents of short-term interest, used for reference, with no evidentiary value
• duplicate copies of documents preserved only for convenience; materials not filed as evidence of business unit/service operations or for their informative value
• modifications and updating of data as part of the running of established electronic software programs, where such processes do not result in the loss of data of continuing value.
• rough notes, calculations or non-substantive drafts created to prepare or analyse other documents
• background materials used to develop a record
• documents or communications that are not needed for the official record, but are useful to an individual for recall of events, activities, and actions
7.2.3 When is an e-mail not a record?

Not all information created, received, or held by the BSA is a record. Further general information can be found in Section 2.2; the main instances particularly applicable to e-mail are:

- personal materials which have no relation to official duties, including e-mails such as “are you going on lunch?” and all-staff social announcements, such as birthday celebrations or charity campaign notices
- RSS feeds and posts to listservs received as e-mail
  - a partial exception is mail on which you have based a specific business decision or activity; e.g., if you post a query to a professional list asking for advice or thoughts on a particular problem / issue, and then receive a response or responses that influence your handling of that issue, you will need to record a reference to the source or, at times, keep the e-mail itself
- ‘circular’ e-mails, such as brochures, conference announcements, unsolicited promotional or sales communications, etc.
- e-mails created, received and maintained by third parties, such as Trade Unions, for whom the BSA provides a hosting service.

7.2.4 A final reminder …

Don’t forget that e-mails are records – be as careful of what you say in them as you would in any other document that will be shared with or seen by others. If you do not want people to know that you think it, don’t record it.

Further information A comprehensive treatment of e-mail as record can be found in Annex J of Managing Electronic Records in Governmental Bodies, produced by the National Archives and Records Service of South Africa.
8 Business Continuity and Preservation of records

The NHSBSA depends on its records and other information to conduct its business. If these are rendered inaccessible either temporarily or permanently, or rendered unusable through loss or deterioration of media and / or content, the organisation will be unable to carry out some or all of its business functions and activities.

Apart from failure to create and keep records in the first place, or inappropriate destruction, or security breaches, the principal causes of records becoming temporarily or permanently unavailable are (a) an incident or disaster that results in damage to the records themselves or to staff being unable to gain access to them; and (b) failure to ensure that necessary maintenance and remedial measures are taken to ensure that the records remain usable over time.

The first of these causes is addressed primarily through the NHSBSA’s Business Continuity Plan, while the second requires an active approach to monitoring and managing records – particularly digital and other electronic records and information, with their greater fragility and instability – throughout their period of active and archival use.

Business continuity and preservation are two of the very few justifications for maintaining copies of records and other information. However, this must be carried out in a systematic and managed way – there should be no unplanned redundancy in the recordkeeping systems.

8.1 Business Continuity

Business Continuity Management (BCM) is a process that identifies the potential impacts of a disruption to an organisation and provides a framework to ensure the organisation can recover from this as fast as possible following a disaster event and help ensure continuity of service to key stakeholders and the protection of the reputation of the organisation. The NHSBSA has put in place a number of Business Continuity Plans (BCPs) and arrangements to help safeguard the organisation against a disaster event and restore operations as soon as possible if such an event occurs. Further information can be found in the Business Continuity Strategy16 and Policy,17 and in the BCPs for each division.

This section focuses purely on the records and information aspects of BCM.

8.1.1 Vital Records

Vital Records are those records which, in the event of a disaster or other disruptive incident, are essential for the recovery of vital operations and the ongoing business of the NHSBSA. While the BSA does not yet have a Vital Records Programme in place, this section outlines some of the principal issues and concerns and some of the ways in which identifying and making emergency provision for vital records can fulfil an essential role in the corporate and local BCPs.

The records identified as vital should be truly mission-critical, as any business continuity or disaster response activity needs to be as lean and focused as possible. The records designated as ‘vital’ may also depend on the context: for instance, an original signed contract may be vital in the sense that it may be the only version acceptable in law, but for immediate operational purposes, a back-up copy might be more essential to enable continued interaction with the other party. While the vital

16 NHSBSABCP002 NHS Business Services Authority Business Continuity Management Strategy
17 NHSBSABCP001 NHS Business Services Authority Business Continuity Management Policy
original document needs to be kept safe from physical harm to ensure its continued existence in the event of, say, a fire – e.g., by being kept in a fire-proof safe – it could be equally vital to have an off-site copy immediately available for business continuity purposes.

Vital records of the NHSBSA include, but are not limited to:

- records necessary to protect legal and financial status
- records identified as necessary to protect assets
- financial records which facilitate continuing solvency and accounting / finance functions
- records that authorise and support the organisation’s most fundamental responsibilities and essential activities
- some records of an administrative nature (key operating procedures, licences, permits, timetables, insurance policies)
- records relating to buildings, doors, safes, sprinklers, alarm systems; personnel lists; building plans;
- vital objects needed in an emergency, but that are not hardware (e.g. building keys)

When the vital records have been identified, they should be listed in a Vital Records Register so that the necessary people can know which records are vital, who creates them, how they are protected and how they can be accessed in an emergency.

Vital records will generally have a fairly limited currency and they need to be regularly replaced with the up to date version. For instance, while the NHSBSA is obliged to keep its financial records for the current year plus 6 years, only the financial records for the past few months are likely to be vital as they will contain the overwhelming majority of amounts payable or owed.

8.1.1.1 Preventive measures

It is good recordkeeping practice to ensure that all records, not just vital records, are secure and as protected from possible threats as is reasonably possible. It is also good practice to audit the situation on a regular basis to ensure that the measures in place remain up to date and effective.

The principal areas where preventive measures may be put in place are:

- staff awareness and training
- following recordkeeping guidance (e.g., by always ensuring that work is held and saved in the appropriate corporate system, so that it is properly accounted for and backed up)
- security of buildings and facilities (e.g., installing and using locks and alarms; regular inspections)
- IT security (e.g. limiting physical access to ICT equipment, protecting data through passwords or encryption; keeping firewall and anti-virus software up to date)
- fire and flood prevention
- storage (avoid storing records in basements or top floors; where building work is in progress; in unsuitable conditions).
8.1.1.2 Extra protection to master vital records on-site

If the master copies of vital records are held on-site, they will need a greater level of protection than that usually possible for non-vital records. Such additional protection can apply to records of any medium and can include:

- locking vital records in a safe or at least a lockable cupboard or desk drawer
- storing vital records in fire- or blast-proof safes, or at least in something that affords additional protection from fire and blasts.

8.1.1.3 Off-site copies and computer back-ups

The most reliable and effective way of protecting vital records is by copying them and keeping them off site in a controlled location. If you can identify and control a location that is far enough away from your office, but can be accessed in the event of an emergency, you should opt for this method of protection.

The ‘official’ copies of records, as mentioned in the introduction to this section, need to be accessible and capable of rapid deployment: for digital records, this means online copies, preferably held on off-site servers. Many vital records will be created or received in digital formats and will be backed up by IT in the normal course of events.

While it is possible to rely on these back-ups in the event of an emergency, the aim of a back-up system is to enable the reconstruction of the entire system in the event of computer failure. Since the back-up records need to be as accessible and searchable as the original, it is unlikely that simple tape back-ups will suffice, unless they can be deployed very quickly and reliably to create a replica of the original records in the same software environment on new servers.

However, if this is the only option for protecting vital records, there should be agreed priorities for restoring the system and records so that the vital records are accessible as soon as possible. This may mean maintaining a separate store of copies of the vital records so they can be easily identified and restored.

It is important to remember that all digital records require not just the records themselves but also operating systems and application software in order to access them in case of an emergency. Systems data and/or software will thus also need to be protected and made available, as will access codes, passwords, serial numbers and other relevant information.

Further information can be found in resources such as Managing Risks and Protecting Vital Records, produced by the UN Archives and Records Management Section (UNARMS).

8.2 Preservation of Records

Many of the NHSBSA’s records need to be kept for significant lengths of time, some for very long periods (e.g. certain HR records need to be kept until the 100th birthday of a former staff member; some records related to buildings must be kept for the lifetime of the building; records of the Board and core committees are kept on-site for 20 years and must then be sent to The National Archives for indefinite retention).

Over time, the materials on which records are made are inevitably subject to deterioration unless measures are taken to preserve them. Some methods of preservation apply to all records, irrespective of format – for instance, poor security,
fire, or flooding will affect any kind of record medium, whether a paper file or a computer disk.

Under normal circumstances, however, non-machine-readable materials such as paper or even microform are generally far more robust than digital materials: not only can they take a lot more punishment and still survive in a usable state, but they are largely safe from the dangers of obsolescence that bedevils electronic records even over the short to medium term.

Parchment, for instance, is an obsolete format, but that does not prevent us from being able to read and use records written on parchment – the data did not need to be migrated to paper once parchment ceased to be produced. However, the same records written to a floppy disk or in an old software format will not remain readable over time – computers are no longer generally manufactured with floppy disk drives, and new software rarely offers full back-compatibility.

Because digital records need more active intervention to ensure their continuing usability, and far earlier in their life, the two classes of record are treated separately below.

8.2.1 Non-digital records
Many of the principles involved in maintaining Vital Records also apply to preserving physical records. The main areas of concern are:

- security
- protection against fire
- protection against water
- environmental conditions
- storage equipment
- equipment for reading / decoding records

8.2.1.1 Security
Records should be protected from unauthorised access – both the buildings in which they are housed and the areas within those buildings where they are kept or stored should have protection and access controls appropriate to the nature of the records

8.2.1.2 Protection against fire
While many of the actions taken to protect records from fire will overlap with general fire protection measures for the NHSBSA's buildings and facilities, extra measures may need to be in place for buildings or areas dedicated primarily to keeping and storing records, e.g. increased fire resistance of doors and other materials, provision of fire-proof containers / safes.

8.2.1.3 Protection against water
Basement areas and attics are particularly susceptible to ingress of water and should not be used to keep or store records if at all possible. Records should, ideally, not be kept in areas where there are water pipes; if they are, the pipes should be lagged. Regular checks should be carried out, including inspection for leaks, dampness or flaky paint/plaster.
**8.2.1.4 Environment**

An unsuitable environment is the biggest single cause of damage to records. Control and observation of temperature, humidity and ventilation within storage areas and regular maintenance of heating / ventilation systems are essential. A stable environment is essential: fluctuations in temperature and relative humidity will cause significant damage.

The most common physical record type is paper, but other forms of physical record, such as microform, film, sound recordings and videos should also be stored in environmentally suitable conditions.

Suitable lighting should be installed, along with protection from harmful light, such as ultra-violet rays coming through windows exposed to sunlight.

**8.2.1.5 Storage equipment**

Records should be stored on shelves and in drawers, cabinets, or other containers in a manner that facilitates retrieval and inspection, and does not crush or cause distortion to the materials.

Storage containers should be appropriate for the record medium, e.g. good-quality strong cardboard boxes for paper files, dust-free metal cans for film. Containers should not be placed on the floor, to give some minimal protection against leakage of water or other fluids.

Large documents, such as maps, should be housed in special storage equipment to ensure that they are not damaged and are readily accessible.

**8.2.1.6 Equipment and aids for reading / decoding / interpreting records**

Physical records are taken here to include non-digital electronic or machine-readable records such as audio and video tape, film, microform, etc. Most of these require mechanical or electrical devices to render them usable or even identifiable. Preservation of the record therefore involves a parallel requirement to preserve the associated technological ‘reading’ devices. If this is not possible, then such records must be managed in the same way as digital records, with a programme in place for migration or conversion to usable formats.

Occasionally, records will be not be readily decipherable without an accompanying ‘key’ – the most extreme example is a document written in code (hardly likely to figure in the NHSBSA’s records), but some records may use terminology or refer to other items or records in a way that is not readily comprehensible without some form of key or index. The latter, too, needs to be preserved alongside the primary record.

**Further information** can be found in resources such as The National Archives’ Standards for the Management of Government Records and the National Archives of Australia’s Preserving Physical Records.

**8.2.2 Digital records**

*Digital Preservation refers to the series of managed activities necessary to ensure continued access to digital materials for as long as necessary.*

---

Digital media are divided into two types: magnetic, where the data is encoded as microscopic magnetised needles on the surface of the medium (e.g., disk or tape); and optical, where the data is encoded by creating microscopic holes in the surface of the medium (e.g., CD, DVD). Records can be stored in several ways:

- **On-line** – on devices such as mainframe computers, networked servers, e-mail and messaging systems, PC hard drives, etc that are available for immediate retrieval and access.
- **Near-line** – on removable media, but remaining relatively accessible through automated systems connected to the network, such as CD jukebox or robotic tape storage.
- **Far-line** – e.g., an on-line index with the records held on disk or tape in off-line
- **Off-line** – on media such as magnetic tape, CDs, and DVDs, not directly accessible through the NHSBSA network and which require human intervention in order to be made accessible to users. This may include copies held as part of the BCP.

Often, digital records start out as on-line records and, as the immediate business need to refer to them diminishes over time, they are moved to near-line, far-line, or off-line storage.

The two fundamental obstacles to maintaining digital records over anything other than the short term are (a) media instability and (b) hardware and software obsolescence / incompatibility. The rapid rate at which storage media degrades and at which hardware and software changes take place means that where digital records are concerned, the definitions of short, long and medium terms must be taken as follows:

- **short term** – up to 3 years after the date of record creation
- **medium term** – 3–7 years after the date of creation
- **long term** – more than 7 years after the date of creation.

This means that, unlike paper records (where ‘passive’ preservation methods such as making sure that they are stored in a suitable environment will often be sufficient for many years after creation), digital records and other information demand active preservation from an early stage in their life – in fact, it is not possible to manage them effectively without having a prior preservation strategy and policy in place.

Since most of the records essential to carrying out the NHSBSA’s activities fall into the medium- or long-term range, active management is required throughout their retention period to ensure that they can be read and used, and that they remain unaltered and reliable as evidence of business activities. This is especially true when records are not stored in on-line systems, which are in everyday use and which will naturally be kept in a usable and accessible state by normal IT maintenance and management. If they are stored on external devices, however, within a very few years the storage media themselves may have been damaged or have degraded, and/or the content may no longer be accessible because the software applications in which they were created are no longer available or supported.

### 8.2.2.1 File format options

Most records are created using specific, proprietary software applications. Over time, these applications will be upgraded or phased out altogether; even with upgrades, there may be no backward compatibility with previous versions. A
common strategy to address this is to convert files from version to version and format to format as the software environment changes.

While non-proprietary formats are the ideal for the long-term preservation of files, they are few in number and each has its limitations: e.g., structure and functionality is lost on conversion to plain text, PDF does not offer full back compatibility. For long-term preservation and use, eXtensible Markup Language (XML) is currently the optimum choice of formats.

8.2.2.2 Digital preservation techniques
The most common approach to preserving electronic records involves a combination of migration and conversion.

- **Migration** is the process of moving files to new media (also known as "refreshing") or computer platforms in order to maintain their value.
- **Conversion** entails changing files from one format from one to another and may involve moving from a proprietary format, such as Microsoft Word, to a non-proprietary one such as a plain text file or XML.

To maintain the integrity of the records, it is important that the process be analysed and monitored to ensure that any changes to the data that may occur in the process are both within acceptable parameters and are fully documented. It is also essential to ensure that any associated metadata remains accessible. Verification techniques, such as checksums, should be used to confirm digital record integrity.

After each transfer it is advisable to perform a test restoration of the data to verify the success of the process and ensure that the digital records are still accessible.

8.2.2.3 Records in business systems
Many digital records are held in business systems such as finance or HR systems; it is important when buying, configuring and maintaining these systems to bear in mind the NHSBSA’s recordkeeping requirements and responsibilities over time. For instance, the capacity to (easily) migrate the records from the system should be specified and built in from the start, as must the capacity to output records no longer required for ‘live’ use to stable, standard-backed preservation formats such as XML, PDF/A, TIFF.

Details of systems, software, and storage environments should be included in records registers and file-plans, as this information is integral to keeping and managing the records over time. It can help identify records ready for migration / conversion, and be of assistance in deciding appropriate digital environments and needs in the first place. The requirements for administrative correspondence that needs to be kept for two years will, for example, be very different from those for the minutes of board meetings, which need be kept for up to 30 years within the NHSBSA and remain in a usable state at that point for transfer to The National Archives, or for pension scheme records that may need to be kept at least up to a member’s 70th birthday or death, and at times well beyond that.

**Further information** can be found in resources such as The National Archives’ Managing Electronic Records in Governmental Bodies, the ICPSR’s on-line tutorial Digital Preservation Management, and the National Archives of Australia’s Digital Recordkeeping Guidelines. An outline of the key concepts can be found in the
Minnesota State Archives Electronic Records Management Guidelines section on Long-Term Preservation.
Appendices

Appendix 1: References

NHSBSA Documents and Publications
These documents are available on the Corporate Policies and Procedures page of the NHSBSA website at http://www.nhsbsa.nhs.uk/2342.aspx

NHSBSABCP001 NHS Business Services Authority Business Continuity Management Policy
NHSBSABCP002 NHS Business Services Authority Business Continuity Management Strategy
NHSBSAIS001 NHS Business Services Authority Information Security Policy
NHSBSAIGM002 NHS Business Services Authority Information Governance Policy
NHSBSARM009 Business Rules for Creation, Management and Disposal of Records on Behalf of the NHSBSA
NHSBSARM012 NHSBSA Corporate Records Retention Schedule
NHSBSARM014 NHSBSA Corporate Business Classification Scheme
** NOT YET APPROVED **
NHSBSARM018 NHSBSA Corporate Business Classification Scheme – Scope Notes
** NOT YET APPROVED **
NHSBSARM017 NHSBSA Data Handling and Storage Policy
NHSBSA Data Classification Matrix

Other Documents and Publications
http://findarticles.com/p/articles/mi_qa3937/is_200605/ai_n17183428/?tag=content:col1

BS ISO 15489-1:2001 Information and documentation — Records management — Part 1: General

Cumbria Constabulary Government Protective Marking Scheme Policy September 2004


Department of Health Records Management: NHS Code of Practice
http://www.dpconline.org/advice/preservationhandbook

Heriot Watt University *Information Security Policy, v1.1 2010*  

Inter-university Consortium for Political and Social Research (ICPSR) *Digital Preservation Management: Implementing Short-term Strategies for Long-term Problems* [On-line tutorial]  
http://www.icpsr.umich.edu/dpm/dpm-eng/eng_index.html

JISC InfoNet [Joint Information Systems Committee] HE Business Classification Scheme and Records Retention Schedule  
http://www.jiscinfonet.ac.uk/partnerships/records-retention-he

JISC InfoNet Records and Information Management  
http://www.jiscinfonet.ac.uk/records-management

Minnesota State Archives *Electronic Records Management Guidelines: Long-Term Preservation*  
http://www.mnhs.org/preserve/records/electronicrecords/erpreserve.html

National Archives and Records Service of South Africa (NARS) *Managing Electronic Records in Governmental Bodies: Policy, Principles and Requirements*, April 2006  

National Archives of Australia *Digital Recordkeeping: Guidelines for Creating, Managing and Preserving Digital Records*, May 2004  

National Archives of Australia *Preserving Physical Records*  

Staffordshire County Council *Records Management Manual*  

The National Archives (TNA) Sustainable Electronic Records: Strategies for the Maintenance and Preservation of Electronic Records and Documents in the Transition to 2004 (Version 1.0), August 2001

UN Archives and Records Management Section (UNARMS) Recordkeeping Toolkit: Section 15 – Managing Risks and Protecting Vital Records

Wisconsin Department of Administration Records Management Basics [presentation].
http://wccawebsite.com/records_mgmt_basics%5B1%5D.ppt?bcsi_scan_3703E4570F27549B=0&bcsi_scan_filename=records_mgmt_basics%5B1%5D.ppt#2
### Appendix 2: Glossary of Records Management Terms used in the NHSBSA

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Administrative records / correspondence</strong></td>
<td>Records or correspondence that are not trivial, but relate more to the ways in which business activities are carried out rather than their substantive activities and decisions – e.g., for a training course, the attendance sheet would be a substantive record, but the booking of trainers, rooms, AV equipment etc would be administrative.</td>
</tr>
<tr>
<td><strong>Archives (1)</strong></td>
<td>A place of deposit for records of historical value, where they are professionally managed, protected and made available.</td>
</tr>
<tr>
<td><strong>Archives (2)</strong></td>
<td>Records that are no longer in use at all for business but have been identified as having long term historical value.</td>
</tr>
<tr>
<td><strong>Audit Trail</strong></td>
<td>Paper or electronic trail that gives a step-by-step documented history of a transaction.</td>
</tr>
</tbody>
</table>
| **Authenticity** | An authentic record is one that can be proven  
  a) to be what it purports to be,  
  b) to have been created or sent by the person purported to have created or sent it, and  
  c) to have been created or sent at the time purported. |

<table>
<thead>
<tr>
<th>B</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Business Classification Scheme (BCS)</strong></td>
<td>The Business Classification Scheme is a conceptual representation of an organisation's business. It describes business functions and activities, and the relationships between them.</td>
</tr>
<tr>
<td><strong>Business continuity</strong></td>
<td>The processes and procedures that an organisation puts in place to ensure that normal business operations can continue during and after a disaster.</td>
</tr>
</tbody>
</table>
**Business records**

Information created, received, and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business.

Evidence that reaches certain agreed standards of business activity; a record can be paper-based, electronic (including e-mail), photographic, an audio or visual recording or any other mechanism by which information can be accessed and shared over a period of time.

**Business rules**

Document that outlines the legal and best practice environment in which the NHSBSA operates. It provides guidelines on when to create (and when not to create) a record, and what makes a record an adequate record as well as other areas of good records management practice of which staff should be aware.

**Classification**

Systematic identification and arrangement of business activities and/or records into categories according to logically structured conventions, methods, and procedural rules represented in a classification system.

*See also Business Classification Scheme*

**Content**

The information recorded in records, of any type and any format.

**Current records**

Those that are in use on a regular basis for business.

**D**

**Destruction**

The process of eliminating or deleting records, beyond any possible reconstruction.

**Disposition**

The range of processes associated with implementing records retention, destruction or transfer decisions which are documented in retention schedules, disposition authorities, or other instruments.

**Document**

Recorded information or object which can be treated as a unit. Refers to all items on which information is recorded, regardless of their status.

**Draft**

A work in progress, which has not yet been signed off or reached stable form. Drafts are still records, and where there is significant variation between drafts, they can be considered substantive. Not to be confused with **Version**
**Electronic Document and Records Management System (EDRMS)**
A software application specifically designed to manage documents and records which are either created within, or saved into, the system.

**Enterprise Content Management (ECM)**
A software application that manages, searches and publishes information from records and documents.

| F | **File** (1) | A set of related records (either written or electronic) kept together  
**n.b.** In this guidance, definition (1), which applies equally to digital and non-digital records, is used throughout unless otherwise specified.  
**See also Folder** |
|---|---|---|
| **File** (2) | (Computing) A collection of data stored in one unit, identified by a filename. It can be a document, picture, audio or video stream, data library, application, or other collection of data.  
**See also Folder** |
| **File-plan** | The recommended way for arranging filing systems, both electronic and paper, for the NHSBSA in order that all staff can find what they are looking for. It is an extension of the **Business Classification Scheme**. |
| **Folder** (1) | An organiser that papers are kept in, to be stored as a single unit in a filing cabinet  
**n.b.** The file (definition 1) occupies a higher hierarchical level than the folder: a file contains folders which in turn contain documents. This is the sense in which the terms are used in this guidance. In computing, the folder contains files (definition 2), which include documents.  
**See also File** |
| **Folder** (2) | (Computing) A logical container of computer files and other folders  
**See also File** |

**Information**
Refers to the content of any document of any status.
<table>
<thead>
<tr>
<th><strong>Information architecture</strong></th>
<th>The design and layout of the points where information exists in an organisation such as databases, web sites, shared drives, etc.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Litigation hold</strong></td>
<td>An organisation's order to preserve any data, records, and materials that may be relevant to current or contemplated litigation or government investigation. Also known as a <em>legal hold</em>, <em>document hold</em>, <em>hold order</em> or <em>preservation order</em>.</td>
</tr>
<tr>
<td><strong>Metadata</strong></td>
<td>Literally means “information about information”; metadata is used to refer to types of information that must be added to a record. Common metadata includes title, date and author but may also include file time or access permissions.</td>
</tr>
<tr>
<td><strong>Preservation</strong></td>
<td>The processes and operations involved in ensuring the technical and intellectual survival of authentic records through time.</td>
</tr>
<tr>
<td><strong>Records</strong></td>
<td>Any type of recorded information, regardless of physical form or characteristics, created, received, or maintained by a person, institution, or organization…. Records are extensions of the human memory, purposefully created to record information, document transactions, communicate thoughts, substantiate claims, advance explanations, offer justifications, and provide lasting evidence of events. Their creation results from a fundamental human need to create and store information, to retrieve and transmit it, and to establish tangible connections with the past. <em>See also</em> Administrative records, Business records, Current records, Semi-current records, Structured records, Substantive records, Transitory records, Unstructured records, Vital records.</td>
</tr>
<tr>
<td><strong>Records Management (RM)</strong></td>
<td>The framework of policy, training, guidance and technical support through which the NHSBSA makes responsible decisions about creating, handling and disposing of its business records.</td>
</tr>
<tr>
<td><strong>Retention schedule</strong></td>
<td>A document that indicates the lengths of time for which the records of business activities are to be retained; these times will be decided by law, guidance or business need. Also known as a disposal schedule.</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>S</strong></td>
<td>ächter records</td>
</tr>
<tr>
<td><strong>Standard Operating Procedures (SOPs)</strong></td>
<td>Each local business area has its own procedures to follow when performing routine business functions, e.g. when to dispose of a record.</td>
</tr>
<tr>
<td><strong>Structured records</strong></td>
<td>Records created within, and that exist mainly as data within, business and database systems. The most familiar general examples include HR systems and payroll systems, ordering and purchase systems (e.g. Amazon), booking systems, etc. Even where the data itself is not limited to certain values, it is contained in a known field and exists in a known relation to other records and components of records within the system.</td>
</tr>
<tr>
<td><strong>Substantive records / correspondence</strong></td>
<td>The contents of substantive records are essential to understanding and maintaining accountability for the business decisions and activities undertaken by the NHSBSA; an example could be a policy document, or the minutes of a meeting, or non-routine correspondence (received or sent).</td>
</tr>
<tr>
<td><strong>T</strong></td>
<td><strong>Technology (ICT)</strong></td>
</tr>
<tr>
<td><strong>Transitory records / correspondence</strong></td>
<td>Transitory records are records of purely temporary or ephemeral value, which contribute towards the creation of other records but need not themselves be kept as part of those records. They include reference material, rough notes, and routine facilitative records.</td>
</tr>
<tr>
<td><strong>U</strong></td>
<td><strong>Unstructured records</strong></td>
</tr>
<tr>
<td><strong>Version</strong></td>
<td>A stable instantiation of a record subject to change over time, which constitutes the definitive record until superseded. Not to be confused with <strong>Draft</strong>.</td>
</tr>
<tr>
<td>-------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Vital records</strong></td>
<td>Those records which, in the event of a disaster or other disruptive incident, are essential for the recovery of vital operations and the ongoing business of the NHSBSA.</td>
</tr>
</tbody>
</table>