London Borough of Enfield

The Corporate Records Management Policy
## Contents

1. Corporate Records Management - Statement ................................................................. 3
2. Corporate Records Management Policy and Purpose .................................................... 4
4. Responsibilities .............................................................................................................. 6
  4.1 Designated Officers ................................................................................................. 6
  4.2 Service Departments ............................................................................................... 6
  4.3 Employee responsibilities ......................................................................................... 7
5. Ownership of information .............................................................................................. 8
6. Filing and Information Classification ............................................................................ 8
7. Record naming conventions ......................................................................................... 9
8. Information Classification ........................................................................................... 10
9. Breach of the Policy ..................................................................................................... 10
10. Links with the Freedom of Information Act ............................................................... 11
11. Links with Subject Access Request ........................................................................... 11
12. Weeding ..................................................................................................................... 11
13. Backups ...................................................................................................................... 11
14. Local Storage ............................................................................................................. 11
15. Archive Storage Area ................................................................................................. 12
16. Retention Schedule .................................................................................................. 14
17. Confidential Waste Policy ......................................................................................... 14
18. Destruction ............................................................................................................... 14
19. Disaster Recovery Planning ....................................................................................... 15
20. Legal Admissibility ..................................................................................................... 15
21. Electronic Storage/Scanning Policy ......................................................................... 15
22. Copyright/Intellectual Property Rights .................................................................. 16
23. Data Protection .......................................................................................................... 16
25. Training .................................................................................................................... 17
26. Bibliography ............................................................................................................. 17
27. Glossary .................................................................................................................... 17

<table>
<thead>
<tr>
<th>Author</th>
<th>Stuart Simper</th>
<th>Classification</th>
<th>OFFICIAL</th>
<th>Date of First Issue</th>
<th>2006</th>
</tr>
</thead>
<tbody>
<tr>
<td>Owner</td>
<td>IGB</td>
<td>Issue Status</td>
<td>FINAL</td>
<td>Date of Latest Re-Issue</td>
<td>30/04/2020</td>
</tr>
<tr>
<td>Version</td>
<td>5.3</td>
<td>Page</td>
<td>2 of 36</td>
<td>Date of IGB Signoff</td>
<td>30/04/2020</td>
</tr>
<tr>
<td>Reviewer</td>
<td>Steve Durbin</td>
<td>Review Date</td>
<td>18/11/2019</td>
<td>Date of next review</td>
<td>30/04/2021</td>
</tr>
</tbody>
</table>
1. Corporate Records Management - Statement

Records Management is a major concern and of exceptional importance to the Council as it provides the means to record our past activities, our current thoughts and our vision for the future. Records and information also allow us to comply with legislation, guidance and standards.

Records provide information to enable us to carry out our business in an efficient manner. It is therefore the personal responsibility of each of us to ensure correct and sufficient information is collected, stored in a suitable medium and retained or destroyed in accordance with the Corporate Retention Schedule.

The retention of records is in many instances a legal requirement, but we must also remember those that follow after us and decide what records must be kept for the historians. This does not mean all information must be retained forever as not only will the majority not be looked at, but also we do not have the capacity to store it.

Because of its importance Records Management should be recognised as a specific Corporate programme within the Council and should receive the necessary levels of organisational support to ensure effectiveness.

Remember, many records are unique and not easily reconstructed or replaced.

Records and information are part of the Council’s memory - they need to be handled in the proper manner.

Chief Executive
2. Corporate Records Management Policy and Purpose

London Borough of Enfield is committed to ensure that as part of its core business, all records (either generated and received by individual employees or third party organisations) are managed effectively and efficiently.

The Council shall store and capture records to ensure compliance with statutory, contractual, evidential, legal, regulatory and London Borough of Enfield requirements.

The aim of the policy is to provide guidance for the creators and users of Council records and information in order to provide the most effective business processes and service delivery, and to meet legislative requirements.

Records are recognized as a vital asset and are owned and managed by London Borough of Enfield. All records are therefore subject to this policy.

Strategy for delivery:

- Establish, maintain and audit documented procedures for identification, capture, indexing, classification, accessing, change control, filing, storage, maintenance, retention and final destruction of all records.
- Store records in such a way that they meet the highest level of integrity and security, are readily retrievable to meet the business needs and are stored within an environment that prevents damage, deterioration or loss.
- Establish a single comprehensive document control environment for all records.
- Appoint a team of London Borough of Enfield staff to deliver and manage all relevant records throughout their life cycle.
- Endeavour, where practical and economical, to create and store records in electronic format.

Compliance with the Policy shall be subject to Management Audit. The responsible person for ensuring compliance with this Policy is the Head of Facilities.
3. Introduction – What Is A Record?

Records can be defined as information, recorded in physical form or medium, received or created by the Council in the course of its business and retained as evidence of its activities or because of the information contained in them will be useful for others. Although not exhaustive, examples of items that can constitute records include:

- Documents (including hand-written, typed, and annotated copies)
- Paper based files
- Computer files (including word processed documents, databases, spreadsheets and presentations)
- Maps and plans
- Electronic mail messages (email)
- Web pages (on either the intranet and internet)
- Faxes
- Brochures and reports
- Forms
- Audio and video tapes including CCTV and voicemail / voice recording systems

**What is Records Management?** Records Management is the development of a programme to control records throughout their life, from creation to ultimate disposal either as confidential waste or as an addition to the archives of the London Borough of Enfield. A good Records Management programme will create a management resource available as long as it is necessary and enable the full use of this resource by the Council.

**What is the scope of this policy?** Although the London Borough of Enfield is increasingly using electronic storage, the Council is not a paperless office. Substantial information is still received, created and retained on paper.

This document covers the Records Management policies implemented for software and conforms to the recommendations of the code of practice for legal admissibility and evidential weight of information stored electronically (BS10008).

The aim of the policy is to provide guidance for the creators and users of Council records and information in order to provide the most effective business processes and service delivery, and to meet legislative requirements.
4. Responsibilities

4.1 Designated Officers

The Chief Executive has overall responsibility but delegates the policy and strategy function to the Council’s Corporate Information Governance Board.

The Head of Legal is Chair of the Council’s Information Governance Board.

The Senior Information Risk Officer (or Owner) is the Director of Law and Governance.

The Council has two Caldicott Guardians – one for Adult Social Care and one for Children’s Safeguarding. A Caldicott Guardian is a senior person responsible for protecting the confidentiality of service-user information and enabling appropriate information-sharing. Guardians play a key role in ensuring that the Council and relevant partner organisations satisfy the highest practicable standards for handling client identifiable information, and for the appropriate sharing of information.

The Corporate Records Manager is responsible for advice on policy and strategy. He or she will also be accountable to the regulatory authorities, the Council and its Members as well as to the citizens of Enfield for compliance with statutory obligations, standards and codes of practice. The day-to-day function is delegated to the Information & Communications Manager.

Specific responsibilities include:

- To establish organisational structures, policies, procedures and standards for the management of records and information.
- To continue to move towards electronic record keeping, and any associated cultural change throughout the Council.
- To measure the performance of service unit staff and record keeping systems.
- To be aware of and make accessible, all known corporate physical and electronic records across the Council.
- To provide Corporate Records Management advice to Council staff.
- To work with managers of information resources to develop a coherent information architecture across the Council.
- To work with accountable stakeholders including the DPA and FOI officers and executive management to ensure record keeping systems support organisational and public accountability.

4.2 Service Departments

The Departmental head will assume responsibility for all information and records within that department. The day-to-day functions may be delegated to a Departmental Data Co-ordinator who will have the following tasks:
• To monitor for compliance with the Corporate Records Management Policy.

• To formally agree which of their Department’s documents are considered sensitive or require special conditions or levels of security.

• To ensure the necessary skills and training are in place or made available to those employees needing them. The training includes Records Management procedures.

• To oversee the effective management of all records within their department.

• To maintain adequate documentation in support of any Records Management decision.

• Maintain an up-to-date information asset register with clear and accurate information

• To ensure asset owners are aware of their responsibilities under the Information Classification Policy

• Ensure records are reviewed annually against the retention schedule and either stored or destroyed securely. This includes archived boxes.

• Ensuring that records (either physical or electronic), when shared outside the Council, are shared complying with law, all Council Information Governance Policies and the relevant information sharing agreements/contact clauses.

• Ensure that all data sharing is suitably covered by Data Sharing / Processing Agreements, and that ICT are made aware of conditions of such Data Sharing / Processing Agreements.

• Ensure that all Data Sharing / Processing agreements are stored in the council’s Register of Information Sharing Protocols.

• Ensure that the Register of Processing Activities and Data Protection Impact Assessments are kept up to date for processing (GDPR Spreadsheets)

• Ensure the secure transit of information (either through secure electronic interfaces or physical movement of paper records)

• In the case of physical records (e.g. children’s case files requested for a legal case) to, where possible, make copies rather than sending the original documentation. However there may be instances where this is not possible and it may be necessary to take advice from Legal Services.

4.3 Employee responsibilities

• Each piece of information or record will have an owner who is responsible for content, metadata (details on author, source, software
requirements if electronic, changes etc), accuracy, safekeeping, destruction and archiving etc.

- In addition to the general responsibility to ensure confidentiality, integrity and availability of records that are held by the Council, are preserved to the highest standard, to create sufficient, appropriate accurate records to support the conduct and business of the Council.

- Records and information in their care must be maintained in such a manner to prevent loss or destruction. Staff must sign out paper documents when working from home or out of the office on business. In addition, laptops and paperwork should be kept separate when out of the office as often as possible.

- Records and information must always be readily available and to this end must not be misfiled, removed from the premises or locked in storage with no access when the employee is away from the premises.

- Employees should be aware of their responsibilities under the Data Protection Act 2018, the Applied General Data Protection Regulation 2016 / EU679, the Freedom of Information Act 2000 and any other relevant legislation. If they are not sure of their responsibilities they should consult their Head of Department or FOI, Information Security representative or the Data Protection Officer

5. Ownership of information

All information received or created by the Council is a common corporate asset and not the property of any individual Department or employee.

The Council is in the process of further development of the Information Asset Register.

6. Filing and Information Classification

It is recommended that information be clearly marked with a date and signature and be filed in date order with the latest date to the top. Papers must be secured within the file cover and not loosely inserted.

Electronic information must be labelled and inserted in an appropriate folder on the PC. This type of information is to be treated for retention, destruction and archiving under the same rules as for paper documents. Do not store information on your PC/laptop hard drive where it cannot be accessed by other staff or would be lost if the laptop was lost or stolen.

Microforms/CD’s should not be left on desks but should be filed in an appropriate container with a suitable index and locked away.

<table>
<thead>
<tr>
<th>Author</th>
<th>Stuart Simper</th>
<th>Classification</th>
<th>OFFICIAL</th>
<th>Date of First Issue</th>
<th>Date of Latest Re-Issue</th>
<th>Date of IGB Signoff</th>
<th>Date of next review</th>
</tr>
</thead>
<tbody>
<tr>
<td>Owner</td>
<td>IGB</td>
<td>Issue Status</td>
<td>FINAL</td>
<td>Date of First Issue</td>
<td>Date of Latest Re-Issue</td>
<td>Date of IGB Signoff</td>
<td>Date of next review</td>
</tr>
<tr>
<td>Version</td>
<td>5.3</td>
<td>Page</td>
<td>8 of 36</td>
<td>Date of IGB Signoff</td>
<td>30/04/2020</td>
<td>30/04/2021</td>
<td>30/04/2021</td>
</tr>
<tr>
<td>Reviewer</td>
<td>Steve Durbin</td>
<td>Review Date</td>
<td>18/11/2019</td>
<td>Date of next review</td>
<td>30/04/2021</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The information that the Council collects and maintains is an essential asset that it relies on to function efficiently and provide excellent services to our residents. Fundamental to this is that we are able to retrieve all the relevant information when needed. This is impossible without a structured filing system whether in electronic or paper form that is organised and managed in a systematic way. A sound filing system will be:

1. Simple and logical so that does not rely on individual officers to self-manage. Does it meet the "temp test" so that a new member of staff or temporary staff with a few basic instructions can easily retrieve information?
2. Accessible to all that require access to the files to do their job (i.e. not kept in personal drives or cabinets or lockers)
3. Papers are arranged in a logical order (e.g. alphabetically/chronological) and or separated into different categories (e.g. HR record could have a section on career progression, pay history, sick absence and disciplinary record)
4. An appropriate indexing/cataloguing system so that paper files can be located easily. For electronic files the use of a consistent naming convention and Metadata so that all relevant information can be effectively retrieved.
5. In the case of paper records an effective system of tracking a files location and whether it is charged out to an officer or in archive store. Also a record of whether files have been reviewed/destroyed.
6. Effective version control is essential to ensure people use the most current information when making a decision.

Under the Council’s Acceptable Use Policy no paper should be left out when desks are not in use, or electronic devices left logged in and unlocked. All paper must be filed away out of hours in locked cabinets and lockers.

The information that the council collects and maintains is an essential asset that it relies on to function efficiently and provide excellent services to our residents. Fundamental to this is that we are able to retrieve all the relevant information when needed. This is impossible without a structured filing system whether in electronic or paper form that are organised and managed in a systematic way.

The Council’s move to SharePoint will help to address effective filing and version control but it will require individuals to take care when naming and labelling documents.

7. Record naming conventions

'File names' are the names that are listed in the computer file directory and which users give to new files when they save them for the first time. Naming records consistently, logically and in a predictable way will distinguish similar records from one another at a glance, and by doing so will facilitate the storage and retrieval of records, which will enable users to browse file names more effectively and efficiently.
Naming records according to an agreed convention should also make file naming easier for staff because they will not have to “re-think” the process each time. Below are some tips for staff:

1. Keep file names short, but meaningful
2. Avoid unnecessary repetition
3. Use capital letters to delimit words or underscores, NOT spaces or hyphens
4. When including a number in a file name always give it as a two-digit number (e.g. 01) unless it is a year or another number with more than two digits (this means that they appear in the correct order in a file list)
5. If using a date in the file name always state the date first ‘back to front’, using four digit years, two digit months and two digit days, e.g.: YYYYMMDD – this again helps ensure they always appear in the correct date order in a file list
6. If using a person’s name in the file list – use the surname first and then their initial or first name
7. Put words like draft and final at the end

Proper labelling of documents -

All documents (except personal letters and publications) should contain the following information in the footer on the first page or cover:

- Author/document owner
- Title/File name
- Version number
- Date of issue
- Number of pages (page x of x)
- Classification (see below)
- Status e.g. draft, final version

Subsequent pages should contain the title/file name, version number and pages (x of x) in addition to the following statement: This is a CONTROLLED document. Any printed copy must be checked against the current electronic version prior to use.

8. Information Classification

Please see the Information Classification and Handling Policy.

Information of all classifications should be disposed of in accordance with the policy.

9. Breach of the Policy

If there is a breach of these rules, staff must report it via the Service Desk.
10. Links with the Freedom of Information Act

A classification does not necessarily exempt the information from a Freedom of Information Act request. However, it will prompt you to consider if an exemption does apply. See the Freedom of Information Policy for further information on exemptions.

11. Links with Subject Access Request

If someone requests to see their personal records, it is important you follow the Subject Access Request procedure in dealing with the request.

12. Weeding

A Retention Schedule is available covering all record types.

It contains details of information to be reviewed, retained or destroyed and at what intervals. Records should be checked regularly to ensure duplicates and non-relevant information is removed. Queries or questions regarding weeding should be directed to the Council's Records manager.

Disposal of information is covered by the Council's Confidential Waste Disposal Policy.

13. Backups

All prime information must be regularly backed up in some manner e.g. electronic or paper with the first format being preferable. The time scale between backups will depend on the importance and financial value of the information. The responsible manager’s decision on the time scale should be recorded. The backup should not be stored in the same office as the original. If the information is irreplaceable then the backup should be stored off-site. ICT and subcontractors back up all information stored on Council systems on a regular basis, but please consult if you have specific requirements; backups are intended for recovery only NOT as records.

14. Local Storage

A locked cabinet should be used to store paper, disks or microfilm records.

Storage boxes are available from the Facilities Management and each must carry a box label (see appendix 3) that must be completed with the following information:

<table>
<thead>
<tr>
<th>Author</th>
<th>Classification</th>
<th>OFFICIAL</th>
<th>Date of First Issue</th>
<th>Date of Latest Re-Issue</th>
<th>Date of IGB Signoff</th>
<th>Date of next review</th>
</tr>
</thead>
<tbody>
<tr>
<td>Owner</td>
<td>Issue Status</td>
<td>FINAL</td>
<td></td>
<td>30/04/2020</td>
<td></td>
<td>30/04/2020</td>
</tr>
<tr>
<td>Version</td>
<td>Page</td>
<td>11 of 36</td>
<td></td>
<td></td>
<td></td>
<td>30/04/2020</td>
</tr>
<tr>
<td>Reviewer</td>
<td>Review Date</td>
<td>18/11/2019</td>
<td></td>
<td></td>
<td></td>
<td>30/04/2021</td>
</tr>
</tbody>
</table>
• Service Department and team name.
• Contact Number.
• List of contents.
• Retention period.
• Scan and destroy paper or scan and retain paper.
• Classification

Which together with the enclosed index, enables such records to be retrieved within the hour within at the Civic Centre and within 24 hours for out stations. There is a computerised database that shows where the boxes are stored, how often they are accessed and whether a file has been returned. Teams may ask for a report to check their holdings.

Review dates should not be used, only destruction dates. They should be selected with care and continually moving them forward is discouraged.

Boxes may be sub-divided so that different types may be stored in the same box. Part filled boxes will not be accepted. Contents should be in the same order as the client provided index.

15. Archive Storage Area

• Documents will only be stored in archive boxes supplied from Facilities Management. Boxes are retained in purpose built storage racks with row and shelf referencing for retrieval purposes.
• Each box must have all paper work supplied by Document Management attached to the box. The index sheet must be placed inside the box for easy traceability.
• Each box is listed on a manual index sheet on entry to the archive with the yellow copies attached to the index sheet.
• Details of all boxes in the archive are inputted to the DMS system, thus providing easy reference and tracking.
• Once entries are completed, the two copies are printed of the Input Form. One copy is attached to the archive box, the other is sent to the customer.
• Once the forms been attached to the box a further check is done to make sure the box is on the correct by row & shelf. This is signed off by another member of staff (not the person who attached the form).

The following procedures are in place for tracking missing files/box.

Checking and tracking mechanisms:

• Check the box was received into the archive via database. All fields can be searched on i.e. search on owners, contact details, department or section.
• If it’s a specific file that’s missing, check the box’s History of Access
• If not successful, check the manual index sheets
• If for any reason the box cannot be traced a full manual search of the archive will take place and the FM Head of Service advised.

Classification of boxes will determine who can retrieve the information. Boxes should be classified according to the highest graded information within it.

All documents must be classified and documents stored within the archive boxes need to marked as noted above. Those with mixed classifications will attract the highest classification control.

Staff are provided with information on how to classify documents. This information can be found on the Enfield Eye.

Managers should not enter into any contracts for other off-site long term storage. Speak to the Corporate Records Manager for advice.

Archiving for the Archivist

Certain items are listed in the Retention Schedule for archiving or passing to the Archivist/Local History Officer. If you are about to destroy any information which may be of use in the future for researchers into the historical events within the Borough and surrounding area, please contact the Local Studies Officer for advice (020 8379 2724). Such day-to-day records may contain valuable historical/genealogical/local history and social science information that may be useful for the studies of social, economic and political issues. They may also have sentimental value to past or present persons of the Borough. Records containing personal information can have a rider on them allowing access to designated officers only, after 30 years or as determined. Other documents to be considered are:

• Records of department operation and structure.
• Information collected by a service group for its own use e.g. customer surveys.
• Information about past activity which would aid future planning.
• Records containing unique information not available elsewhere e.g. burial records.
• Information about policy/decision making e.g. Committee reports and Minutes.
• Records dealing with external involvement e.g. Central Government, Trade Unions, etc.
• Records of research and development.

Retaining whole series of records would be high on space usage, so a limited number should be selected either by choice, random sampling or systematic sampling methods.
16. Retention Schedule

Retention scheduling is the process of documenting a record’s value in the terms of the length of time it should be retained. Its objectives are to:

- Personal data should only be retained where there is a legitimate need.
- Dispose promptly of those records whose retention period has ended.
- Retain records that are no longer current, but which need to be kept for some time for statutory or audit purposes.
- Preserve records that have a longer-term archival/historical value.
- Enables good record keeping practices.
- Meets management’s information needs.
- Establishes a systematic programme to determine value of records before destruction.
- Saves time by reducing the volume of files to be searched for.
- Avoids legal problems.
- Promotes efficiency by focusing on those records that are important.
- Saves space by removing non-current records from office accommodation to storage.
- Identifies valuable records for archival preservation
- All services should review and update their list of archives every year.

The Council has a Corporate Retention Schedule that should be followed by all Departments. It is managed by the chair of the Information Governance Board who is responsible for all additions, deletions and amendments. Internal Audit are consulted on all changes.

17. Confidential Waste Policy

The Council has a policy to ensure that the security of waste documents is upheld until pulping (see Information Classification and Handling Policy). This Policy includes the issue of destruction certificates.

18. Destruction

Once it has been decided that information can be destroyed paper records may be disposed of via the confidential waste system. Electronic data on discs and microfilm can also be destroyed. The Records Unit can arrange this. There are additional systems available for the destruction of such items as blank cheques and items of the highest sensitivity.
19. Disaster Recovery Planning

Every Department should have a Business Impact Analysis Plan in order to protect information and to promote maximum recovery. In the case of electronic records there may be a need for duplicate hardware and software.

20. Legal Admissibility

In order to ensure the storage medium is acceptable in a court of law and carries the same weight of evidence as the original paper version all microforms should comply with the appropriate British and International Standards.

Electronic storage should follow the recommendations of BS10008 via the code of practice BIP 0008 Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically - Issued by the British Standards Institution. BSI has issued a workbook to compliment the Code of Practice. Completion of this will show with which parts of the Code you comply.

21. Electronic Storage/Scanning Policy

E-mail and information stored on a PC and used to facilitate the performance of Council work is a corporate asset and a critical component of the Council’s communication system. Such information may therefore be used in court of law in the same manner as information stored on paper or microfilm.

For these reasons the information should be dated and assigned a responsibility e.g. it should show who the author is. Filing should follow the same standards as for paper and each folder should show the same information as for a paper file.

There should be consistent naming conventions for records. The Council is developing a common naming convention.

Electronic records must be protected from physical and intellectual damage (editing, version control). Their use must be tracked and managed, using the Information Classification Policy.

Emails that are required to be kept under the retention schedule should be stored in the relevant case management system/shared drive and not in the email systems.

No tape or disc should be thrown away or reformatted without being checked for material needing to be retained by legislation or for historical research. Consider creating an archive disc or tape.
Services are responsible for data cleansing systems and ensuring the retention schedule is applied to electronic data.

Document imaging - should be considered if there is a need to:

- Automate document-based workflow.
- Integrate document and data processing.
- Manage large volumes of active documents.
- Provide multi-access document handling.
- Provide on-line document access.
- Provide printed copy locally.
- Control access to document retrieval.

A back-up copy may still be needed where there is a long term storage need especially for information that is intended for the archives. This is because the hardware to read the disc version may not be available in years to come.

### 22. Copyright/Intellectual Property Rights

This is a very complicated legal area and the work of others outside the Council should not be copied without their permission. Work prepared on the Council’s equipment during working time is most likely to be copyright of the Council. This includes e-mail.

### 23. Data Protection

The Data Protection Act 2018 took the General Data Protection Regulation 2016/EU679 into UK law and amended it for derogations and UK interpretations. This, along with a number of other regulations and case law is now referred to as the “Data Protection Law”.

This covers all information referring to natural living persons regardless of format (paper/film/electronic/disc) and reference must be made to the information available from the Data Protection Officer. Please also refer to the Council’s Data Protection Policy, and online training.

### 24. Freedom of Information Act 2000

This legislation opens the majority of the Council’s information to the public. Employees need to be aware of the Council’s procedures and of the exemptions. More information is available from the Council’s FOI Officer. Please also refer to the Council’s Freedom of Information Policy.
25. Training

All Council employees are involved in creating, maintaining and using records and it is important that everyone understands their Records Management responsibilities as set out in this policy. Managers will ensure that staff are appropriately trained.

26. Bibliography

The following list is not exhaustive and if there is doubt, advice should be sought from the Legal Department.

- BSI PD 5454 Guide for the Storage and Exhibition of Archival Materials
- Copyright, Designs and Patents Act 1988
- Data Protection Act 2018 and the Applied General Data Protection Regulation EU679/2016 (GDPR) created by the act
- BS10008 Evidential weight and legal admissibility of electronically stored information
- BIP 0008 Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically
- Electronic Communications Act 2000
- Employment Rights Act 1996
- European Directive on Environmental Information
- Freedom Of Information Act 2000 (FOIA)
- ISO 154489 Information and documentation-Records Management
- Local Government Act 1972
- Freedom of Information Code of Practice issued under s.45 of the FOIA by the cabinet office.
- Public Records Office Act 1958 and 1967

27. Glossary

Archive
The retention of information for further and possibly other use after the business use has finished

Capture
The act of registering a document or transaction as a record and storing it in a record keeping system. Part of this process will usually include adding metadata to the record.

Classification Scheme
Systematic identification and (usually hierarchical) arrangement of business activities, documents, records and folders in to categories in order that records can be logically stored or grouped together for efficient organisation sharing and retrieval.
Document

Often defined as ‘any recorded information or object that can be treated as a unit of filing’ thus a letter, form or report can be considered a document. A document can be described as a record once it records activity. However, many documents exist in their own right. For example an empty printed form is a document; whereas once it has been completed it can be registered as a record since its contents record an activity and give it added meaning.

Electronic Record

A record held in electronic form.

Evidential Weight

The amount of importance or trust placed by the Court on the evidence being presented.

Filing System

A collection of information regardless of storage format.

Folder

A set of related electronic records and physical records; folders can be electronic or physical and can be associated with metadata.

Inventory

A list of file series being used within a Team.

Meta data

Data describing the context, content and structure of the record (s).

Physical record

A record that is permanently held and managed in a non-electronic format. e.g. paper, video, microfilm, soil sample, audiocassette or CD. A printed electronic record or document is not necessarily a physical record.

Record

Any evidence in physical or electronic form of something that was communicated or decided, or action was taken. Records can be any of the following:- records created by the Council in the course of its business; ‘Public records’ (for example records of courts, coroners, hospitals and prisons) held on behalf of central government; records given to or purchased by the Council; or deposited with the Council - normally on indefinite loan. A record should be able to support the needs of the business to which it relates and be used for accountability purposes.
**Record keeping systems**  
A system or process (either manual or automatic) that captures and stores *physical or electronic records.*

**Register**  
The act of designating a document within a record keeping system as a physical or electronic record. Once registered as a record the content of the record (and its metadata) must not be changed. You can have different versions but each version or amended copy must be registered in its own right to enable the audit trail to be followed.

**Series**  
A collection of files relating to common information related by subject or usage