Birmingham City Council

PROCEDURE

RECORDS MANAGEMENT MANUAL

If you have any enquiries about this Manual please contact Records Management Service on records.management@birmingham.gov.uk

Standard Owner:	Malkiat Thiarai Head of Corporate Information Management
Author	Records Management Service
Version:	2.0
Date:	23 January 2014
Classification:	NOT PROTECTIVELY MARKED

CONTENTS

Introduction

Responsibilities

Creation

Arrangement and Description

Electronic Records

Storage and Maintenance

INTRODUCTION

WHAT IS A RECORD?

Records can be described as the information that you create and receive in the course of your work which provides evidence of actions, decisions and transactions.

The formal definitions from ISO15489, the international standard on records management, are:

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

Records Management: field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records; including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records.

Records are a means of providing evidence of activities which support the business and operating decisions of the council, and these can be in any format. Examples of different types of records include:

- CCTV recordings
- Emails
- Property files
- Staff files
- Minutes
- Financial records
- Diaries

WHAT IS NOT A RECORD?

Not all information is necessarily a formal record. Types of information that are not records include:

- information relating to personal or social activities
- books, magazines, periodicals etc. held for reference purposes
- stocks of printed publications and publicity materials retained for supply purposes
- duplicate copies of records held for convenience or personal reference and where the master set of the records has been identified and retained elsewhere.

CHARACTERISTICS OF A RECORD

Implementation of good records management procedures and practice should result in authoritative records. That is the records will exhibit the following characteristics:

Authenticity

An authentic record is one that can be proven to:

- be what it purports to be
- have been created or sent by the person purported to have created or sent it
- have been created or sent at the time purported.

Reliability

A reliable record is one:

- whose contents can be trusted as a full and accurate representation of the transactions, activities or facts to which they attest
- that can be depended upon in the course of subsequent transactions or activities
- that is created at the time of the transaction or incident to which they relate or soon afterwards, by individuals who have direct knowledge of the facts or by instruments routinely used within the business to conduct the transaction.

Integrity

The integrity of a record refers to its being complete and unaltered. To have integrity:

- a record should be protected against unauthorised alteration
- any authorised annotation, addition or deletion to a record should be explicitly indicated and traceable.

Usability

A useable record is one that can be located, retrieved, presented and interpreted. It should be:

- capable of subsequent presentation as directly connected to the business activity or transaction that produced it
- linked to information that provides an understanding of the transactions that created and used them
- possible to identify a record within the context of broader business activities and functions.

WHY DO WE NEED RECORDS?

The Council needs records for various reasons including:

- to be able to deliver consistent services
- to make decisions based on sound evidence
- to meet regulatory and legislative requirements
- to be accountable
- to protect the rights of the Council, its citizens and clients, employees and stakeholders
- to provide protection and support in the litigation process.

KEY DRIVERS FOR RECORDS MANAGEMENT

Good records management is essential to ensure that the council can comply with its legislative responsibilities and can act as a driver for business efficiency. Effective management of records and information brings the following benefits. It:

- increases efficiency by enabling better use of resources
- improves openness and accountability
- helps achieve and demonstrate compliance with legislative and regulatory requirements
- enables the protection of the rights and interests of the council, its employees and citizens
- supports joint working with partners and the exchange of information across the council
- provides institutional memory.

Poor records and information management creates risks for the council, such as:

- poor decisions based on inaccurate or incomplete information
- inconsistent or poor levels of service
- financial or legal loss if information required as evidence is not available or cannot be relied upon
- non-compliance with statutory or other regulatory requirements
- failure to handle confidential information with an appropriate level of security and the possibility of unauthorised access or disposal taking place
- failure to protect information that is vital to the continued functioning of the council, leading to inadequate business continuity planning
- unnecessary costs caused by storing records and other information for longer than they are needed
- staff time wasted searching for records or considering issues that have previously been addressed and resolved
- loss of reputation as a result of all of the above, with damaging effects on public trust.

LEGAL & BUSINESS FRAMEWORK FOR RECORDS MANAGEMENT

The legal and regulatory environment in which the Council operates is incredibly complex and there is not one single piece of legislation that clearly specifies the arrangements the Council should have in place for managing records.

Some legislative requirements such as health & safety will be generally applicable throughout the Council. However, other legislative or regulatory requirements will be specific to certain service areas. The legal and regulatory environment of the service area should be considered when developing records management procedures and making decisions about which records need to be created and maintained.

Failure to manage records properly could lead to the Council failing to comply with legislation that relates to information such as the Freedom of Information Act and the Data Protection Act.

RESPONSIBILITIES

DIRECTORATE

Strategic Directors are responsible for supporting the application of the records management policy and standards throughout their Directorate. This includes ensuring that line managers know their responsibilities and those procedures which comply with corporate policy and standards are in place.

SERVICE AREAS

Directors, Assistant Directors, Heads of Service, Senior Managers, Department Heads are responsible for:

- ensuring systems which are developed for the purpose of creating and capturing records enable records to be stored, retrieved and disposed of as necessary
- ensuring that full and accurate records are created and captured by staff into the recordkeeping system
- developing and operating records management procedures, covering both electronic and hard copy records that comply with the records management policy and standards
- ensuring employees, including contractors, consultants and volunteers employed to undertake council business follow procedures for the management and storage of electronic and hard copy records including the development of verification procedures for monitoring compliance with procedures
- ensuring appropriate resources are in place to enable compliance with the records management policy and standards
- communicating records management procedures.

It is important that as staff for the Council understand that information and records are assets of the organisation and as such need to be actively and properly managed. All staff will have varying degrees of responsibility for creating records to support business activities and decision-making processes in which they are involved. Staff should have the necessary skills and knowledge to fulfil their records management responsibilities. Line managers are responsible for identifying any necessary training or support.

CONTRACTED OUT SERVICES / PARTNERSHIP WORKING

Agreements and contracts relating to service provision on behalf of Birmingham City Council and/or where the Council is working in partnership should clearly define and document responsibilities for the management of records.

PROJECT WORKING

Where records, such as project records, are created as the result of an activity of a temporary nature the senior manager for the activity is responsible for ensuring that the records are created and managed in accordance with records management policy and standards. This includes ensuring the necessary resources for the management of the records are available and that ownership of the records is clearly defined and documented if the records need to be retained once the activity has ended.

RECORDS MANAGEMENT SERVICE

The Records Management Service (RMS), based in Performance & Information within the Corporate Resources Directorate is responsible for:

- definition of corporate records management policy and standards
- promotion of compliance with corporate records management policy and standards
- development of retention schedules and business classification schemes
- provision of records management advice and development of best practice guidelines
- provision of records management advice on the specification and implementation of computer systems where they generate and store records
- identification and reporting on information risks through a programme of information audits
- development and provision of relevant training
- management of corporate records storage including administering access to the service and the disposal process
- management of the corporate confidential waste contract
- development of strategies for the permanent preservation of selected records in partnership with the Archives & Heritage service.

CREATION

IDENTIFYING INFORMATION TO BE CREATED AS A RECORD

Each service area within the Council must decide what records it needs to create and maintain. This decision is influenced by the legal and regulatory environment in which a department operates and the specific nature of the business that it undertakes. However records should be created to:

- provide evidence of policy, decisions, actions and activities
- provide evidence of compliance with rules, regulations and legislation appropriate to the organisational context to ensure the Council’s accountability
- allow employees and their successors to assume their roles and responsibilities
- act as an information source to guide future actions taken by the Council
- keep track of the progress of a project or process.

Having guidance in place stating which documents should be captured as a record provides a level of consistency. However, it is not always possible to identify every type of document that may be held and there may be instances where staff are required to make a judgement about whether certain types of information are important enough to be captured as a record or not.

WHEN SHOULD RECORDS BE CREATED?

Records should be created at the time of the transaction to which they relate, or as soon as possible afterwards. An example of this is the creation of minutes of a meeting following closure of the meeting.

Records should also be created by individuals who have direct knowledge of the facts or experience of the matter that is being recorded, or by equipment/systems routinely used within the business to conduct the transaction.

MANAGING INFORMATION WHICH IS NOT A RECORD

All information held by the Council may be subject to a Freedom of Information request whether it is considered to be a formal record or not and should be managed with a view to the possibility it may have to be made publicly available. If requested information is destroyed before a request has been received then you can say that you do not hold it, but should explain why it was destroyed. However, destroying information outside normal procedures in order to avoid disclosure may be a criminal offence.

All staff can create and hold information which will not be kept as part of the Council's formal records. Examples of this type of information include:

- draft notes of meetings which don't require to be formally minuted where decisions will be made at formally minuted meetings
- information held for personal reference and information such as research notes and note books which are likely to cover a mix of activity
- drafts of documents where the final version has been finalised and approved and there is no need to evidence any significant changes in approach.

Information not kept as a record still needs to be managed appropriately. General principles include:

- try to keep personal and reference information separate from official records as this avoids the need to weed files later
- file information regularly
- review information regularly to check whether it still needs to be retained
- destroy information when it no longer has any value as reference material or when it is superseded
- information that is confidential or includes personal information should be destroyed securely and confidentially.

DUPLICATE RECORDS

Avoid creating duplicate copies of the same record. The master copy should be identified and captured into a shared record keeping system. Where standard letters and forms are required shared master templates should be created and used to ensure consistency of recording and to prevent loss, alteration or the accidental disclosure of information.

Records to be kept should be captured into a record keeping system. The system, whether paper or electronic, should include a set of rules for referencing, titling, indexing and where appropriate the security marking of records. These should be easily understood and should enable the efficient retrieval of information.

DESIGNING SYSTEMS FOR CREATING AND CAPTURING RECORDS

Records should be captured in systems which enable them to stored and retrieved as necessary. Records systems should meet the following criteria. They should:

- be easy to understand and operate – this should be considered when designing and developing a new system
- enable quick and easy retrieval of information
- be set up in a way that enables records to be destroyed in line with retention policy as a routine process
- protect records from unauthorised alteration, movement or copying
- provide the required levels of security
- enable relevant audit trails to be produced.

Records systems should be documented to facilitate staff training, maintenance of the system and reconstruction in the event of an emergency.

ARRANGEMENT AND DESCRIPTION

WHAT IS A FILING SCHEME?

A filing scheme specifies how records are to be organised and maintained once they have been created or received by an organisation. Having an agreed filing scheme in place will mean that there is a consistent and agreed approach to the way that information is managed within your service area.

A single filing scheme should be used for paper and electronic records, so filing cabinets, shared network drives, electronic document management systems and email all mirror each other. This means that information can be quickly located as it is stored in the same folder regardless of the format that it is held in. A filing scheme is sometimes also called a business classification scheme. The use of a classification or filing scheme is a requirement of the International Records Management Standard BS ISO 15489.

The main benefits of setting up a filing scheme are that:

- it should be quicker to find information and share this with colleagues
- all of the information relating to a particular activity will be found in one place
- it can preserve the business context within which records are created
- it will be easier to apply decisions on how long different types of records are to be kept for and to manage the disposal of them
- it should help to prevent information from being duplicated and confusion occurring over which is the most up-to-date version of a record
- it will allow security permissions to be applied effectively

HOW DO YOU DESIGN A FILING SCHEME?

Each service area is responsible for developing and implementing a filing scheme – also known as a file plan – for the records that it holds. Before deciding how to arrange your filing scheme you will need to carry out a survey in order to identify your main business activities and the types of records that your department creates as a result of them. This information can then be used to identify the scope of the scheme and the most appropriate way for it to be organised.

Designing the file plan can be a time intensive process but it is an essential part of ensuring that records can be effectively managed. To design an effective structure you will need to have a good understanding of your business area.

Filing schemes can be arranged:

- alphabetically: each folder is arranged in alphabetical order e.g. by client surname
- numerically: each file is given a unique reference number and then arranged accordingly. This is effective if your files are assigned a unique job, project or case number
- by subject: this involves reviewing the subject matter of a file, although it can be difficult to identify the relevant folder if a file relates to more than one subject
- by function/activity: based on the functions and activities carried out by your department.

It is recommended that you arrange your filing scheme based on a combination of function and subject so for example all of the finance or human resources records are grouped together. A file plan based on the ***functions*** and ***activities*** of your service area is likely to be much more effective as functions and activities remain much the same over time and will be unaffected by changes in organisational structure. Although the same department may be known as Human Resources, Personnel or Staff Development and Welfare over a number of years, the functions and roles it carries out will largely remain constant: recruitment, appraisal, training, disciplinary procedures etc.

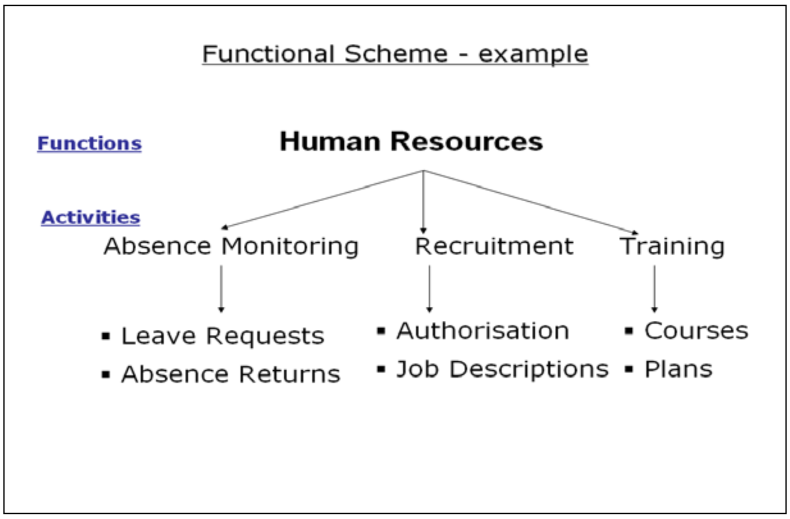
By basing your filing scheme on your service area's underlying functions and the activities that are carried out to achieve them, then a far more stable system will be developed. It will also be easier to navigate for those who do not have a detailed knowledge of your service area as it does not rely on obscure department specific names or acronyms. A functional approach also ensures that records relating to a particular activity are all in one place and helps to explain the relationship between the records.

To create a functional file plan, the first task is to identify what your service area is responsible and accountable for doing i.e. its functions.

Functions represent the broad responsibilities and work areas of the Council; they are what the Council does. Functions may be derived through legislation, policy or programme development, or they may represent a set of tasks or activities that result in goods or services which the Council is expected to provide e.g. finance, human resources, health and safety. Functions are the first level of the filing scheme.

Activities are the major tasks performed by an organisation to accomplish each of its business functions e.g. financial planning, budgeting, recruitment and policy development. Depending on the nature of the transactions involved, an activity may be performed in relation to one function, or it may be performed in relation to many functions. Activities are the second level of the filing scheme.

The relationship between functions and activities in a functional file plan



The Corporate Retention Schedule can provide a starting point when developing a functional filing scheme as it will help you to identify the functions and activities relevant to your service area and the type of information that is created as part of the business activities. The structure of the retention schedule has been based on the Local Government Classification Scheme and amended to cover the main functions and activities carried out by the Council. The headings used in the Corporate Retention Schedule at level 1 represent the main functions e.g. finance, health and safety and human resources. The headings used at level 2 represent the main activities identified within these functions. The retention schedule can be accessed on Inline http://inline//retention.

Making the filing scheme easy to use is critical to its success. It is best to try to limit the number of levels (or folders) to avoid discouraging users with a time-consuming and complicated structure. If you have too few levels then you will end up with a high volume of documents at each level making it difficult to locate relevant items. A filing scheme should ideally consist of a 3 or 4 level hierarchy, with the lowest levels being individual files and the highest broad functions.

A spreadsheet should be used to record the file plan structure and each of the record types contained within it. This will need to be updated when any changes are made. Retention requirements should be included within the scheme so that everyone within your service area knows how long to keep the records for and so that the records can be destroyed on a regular basis.

ADMINISTRATON AND MAINTENANCE OF THE FILING SCHEME

Procedures will need to be developed for using the filing scheme and training provided to staff. Responsibility should be assigned to an individual member of the team for monitoring, reviewing and updating the filing scheme to ensure that it continues to meet your service area’s needs.

MANAGING CASE FILES AND SUBJECT FILES

Case files contain material relating to a specific action, event, person, organisation, location or product. A case file documents the history of a case from beginning to end and is usually filed by name or unique reference number. For example, a personnel file is a case file as all of the information in the file relates to one individual whilst they are employed by an organisation. The creation and management of case files takes place across the Council in areas such as housing, benefits and social care.

Subject files contain documents that relate to the same topic or subject matter. They are created because it is usually easier to retrieve records relating to a particular subject when they are grouped together. For example a Human Rights subject file may contain sample policies, advice from experts, newspaper articles and decisions from the Human Rights Commission.

The management of both case and subject files requires particular consideration in order to ensure that effective records management practices are applied.

If you have access to electronic document and records management systems (such as e-records) then you should save any case files that you create to this system. This is the most effective way of managing electronic case files as the records can be easily searched for and individual retention requirements can be applied to the different types of information contained within a file.

When an electronic document management system is not available then case and subject files held electronically should be saved to your service area’s shared network drive. The case files can be saved within your main filing scheme in a separate folder. Additional sub-folders may need to be created within each individual case or subject folder to distinguish between the different types of information held relating to the subject and to help improve information sharing and retrieval.

Case and subject files held in paper format should be filed together as distinct record types and arranged by name or unique reference number. A number of files relating to each case may need to be created. Older files (history files) relating to a case should be ‘closed’ and removed from the main filing system when they no longer need to be accessed on a regular basis. They can be sent offsite for storage with the Council’s approved contractor.

When information relating to a case or subject is held in both paper and electronic formats then cross references should be made between the two systems so that your service area is aware of exactly what is held in each format. If this is not done then there is the risk that information may be duplicated and decisions may be made on out of date or incomplete information.

Case and subject files can often contain different types of information that have different retention requirements. It can be time consuming to weed and sort case files by document or information type so the longest retention period should be applied to the files. Information on how long to retain case and subject files for can be found in the Corporate Retention Schedule.

WHAT IS METADATA?

Metadata is information that describes an object’s structure, context, content and management through time. By describing information and records then users know what they are about, understand their context and purpose, and can easily find them when they need to.

Metadata relates to all records regardless of the format that they are held in including paper, electronic, video, photographs and web pages. For example, a digital image may include metadata that describes how large the picture is, the colour depth, the image resolution and when the image was created. A text document's metadata may contain information about how long the document is, who the author is, when the document was written, and a short summary of the document.

Metadata for records in any format should be kept in such a way that it remains reliable and accessible for as long as it is required, which will be for at least the life of the record.

Some examples of metadata are:

- title
- author or originator
- any registration number or other unique identifiers e.g. case or project number
- date created or received
- subject matter
- format
- history of use
- security marking
- retention and disposition actions required.

The capture and maintenance of metadata should occur as part of normal business and records management processes. Metadata should be gathered and associated with each record at or before the point of capture.

The basic national standards with which the Council needs to conform are the e-Government Metadata Standard (e-GMS) and the Dublin Core. These are the standards for Metadata which contain mandatory rules for recording information controlled by the Council.

WHY IS METADATA IMPORTANT?

The use of metadata means that important details about the information that your service area creates is recorded in a structured way, and provides valuable context to that information. It also:

- provides a tool for the control and management of records
- provides a way of confirming the authenticity and integrity of records
- assists in the identification, retrieval and delivery of records to authorised users.

Without metadata, information and records have no context, making them difficult to find, retrieve and use.

METADATA WITHIN AN ELECTRONIC DOCUMENT MANAGEMENT SYSTEM

Within an electronic document management system, metadata is used to provide data about records and folders i.e. details on how long to keep a record or to specify who can access a record. This metadata is often used by the system to manage functions such as access controls and disposal rules. Metadata can either be entered by users when a record is captured into the system or automatically applied to records when they are created from predetermined elements such as classification, retention and security. If you have access to an electronic document management system or other business system then the metadata will already have been defined according to the processes followed by your service area.

HOW SHOULD DOCUMENTS AND FOLDERS BE NAMED?

Giving documents and folders meaningful and easily recognisable titles (or names) will enable you to retrieve your records quickly. A good file name will also help your colleagues to readily identify relevant information without having to open the document or folder, therefore improving information sharing. The use of consistent standardised file names will also help to make searching more efficient. Standardising commonly used elements of document and folder names will help to avoid confusion and improve searching.

Common rules for standard file names include:

- use the format YYYYMMDD for dates as this will sort records in date order on the computer
- transpose second and first names for personal names e.g. Smith John
- when using a numbering system add the number before other title elements e.g. project number then project title

Avoid subjective terms

- Make sure that the terms you use will make sense to others and yourself at a later date
- Avoid terms that may potentially have more than one meaning and could cause confusion
- Don’t use terms which are likely to change, for example a document entitled ‘current organisation chart’ will become outdated.

Make it meaningful

- Avoid abbreviations and acronyms which are not in common usage and are unlikely to be understood by others
- Avoid using your name to title folders and documents (for example Dave’s folder) as other staff may not be aware of everything you do, especially if you leave the council
- Do not use terms such as miscellaneous as it will quickly become a dumping ground for everything and difficult to manage.

Be concise

- Include only the important information in the document/folder name
- Shorter names will help you and others identify relevant information more quickly.

Standard file naming conventions should be introduced within each division and the ‘footer’ facility used on all documents created to record the file name.

NAMING EMAILS

You will need to develop specific guidance for the naming of emails that are to be saved to the shared network drive. When emails are captured from Microsoft Outlook into a file system they are automatically named using the text in the ‘Subject’ field of the email and as a result, the prefixes ‘RE’ for replies and ‘FW’ for forwarded emails may be retained. These prefixes need to be removed to ensure that the title of the record is explicit to the purpose and content of the captured email. This is particularly important if several emails are captured as part of a longer communication. If all related emails are given the same title then the context and reason for capturing the email will be lost.

WHAT IS VERSION CONTROL?

Version control is the management of multiple revisions to the same document. The different versions created are numbered to allow the process to be monitored. This means that the most up-to-date version of the document can be easily identified. A clear audit trail is also created which tracks the development of a document and identifies earlier versions when needed.

The use of a version control system helps to prevent decisions from being made on out of date information that is believed to be current. It is important to use a version control system if you are working on a collaborative document with a number of contributors and/or frequent revisions, for example a consultation response, to demonstrate the changes that have been made.

WHICH VERSION CONTROL SYSTEM SHOULD BE FOLLOWED?

The version control numbering system adopted by your service area should track documents from the first draft to the most recent version. The system should demonstrate the major and minor revisions that have been made to a document. In the major/minor system the first number represents a significant change to the content and the second number represents a smaller change.

For example

- Survey Report 0.1, 0.2, 0.3, and so on for all draft documents
- Survey Report 1.0 (final amendment/first version)
- Survey Report 1.1, 1.2 and so on for subsequent amendments to the first version
- Survey Report 2.1 (final amendment/second version)

For more formal documentation that is going to be subject to legal or regulatory requirements then a version control table can be used as an audit control and to demonstrate when particular changes have been made. The table can either be included at the start of the document, or as a separate document. The version control table should include the following details:

- Version number
- Purpose and/or detail of the change
- Author of changes
- Date of change

Example of a version control table

Version number	Purpose/Changes	Author	Date
0.1	Initial draft shown to all Managers	John Wake	19/11/2012
0.2	Incorporating suggestions from all Managers	Mary Smith	07/01/2013
0.3	More detail added after meeting with Head of Service	Jane Doe	24/01/2013
1.0	Final draft approved by the Team	Jane Doe	04/03/2013
1.1	Correction of spelling error in paragraph 28	Mary Smith	16/04/2013

It is common practice for draft versions to be destroyed once the final version has been approved. However draft versions may need to be retained in the following circumstances;

- if it is the subject of any Freedom of Information (FOI) enquiry
- if it shows the thought process and discussion which led to the formulation of a decision or policy and proves useful from a ‘lessons learnt’ perspective

ELECTRONIC RECORDS

ELECTRONIC DOCUMENT & RECORDS MANAGEMENT SYSTEM (EDRMS)

EDRM system is a specialised business information system designed to manage a range of electronic contents e.g. documents and records from word documents, emails, scanned documents and website. Example of EDRM system used within the Council including:

- Voyager
- GIS (geographical information systems)
- eRecords
- People Solutions
- SharePoint
- Fatwire and websites
- Architectural drawing systems

EDRM system can assist to manage the information through its ability to:

- assists in compliance with standards, legislations and audit requirements, particularly Data Protection and Freedom of Information Act
- improves information request turn-around and decision making
- promotes information sharing and reuses records through simultaneous access of documents by multiple users in multiple locations
- protects records from loss and destruction
- enables flexible / mobile working
- can make significant records storage savings and improves security access
- achieves complete records by the system's ability to manage a variety of documents formats including emails.

The format of an electronic document does not change the fact that it is a record and must be managed throughout their life-cycle from creation to destruction, adhering to Council's Records Management Policy. It is necessary to ensure that the correct access, security and retention dates have been applied to all types of records held within the EDRMS.

MANAGING RECORDS ON THE SHARED NETWORK DRIVE

The majority of electronic information created and received by service areas within the Council should be saved to the department's shared network drive. This is particularly important if the information needs to be shared with or accessed by anyone else within the department.

Confidential information can be stored on the shared network drive in a password protected folder in order to restrict access to it. Any personal information that other members of the team do not need to have access to e.g. notes from meetings with manager or PDR preparation work should be saved to your own personal space on the shared network drive.

Shared network drives should be used to store records rather than removable media such as CDs, DVDs or USB memory sticks. Information stored on removable media is not only less secure and more prone to being lost but is also far more susceptible to becoming obsolete.

Managing electronic records without using EDRM system requires a formal and stringent control against any risk of alteration or deletion. This is to ensure that a record's integrity is not compromised and its authenticity remains reliable whenever required. Therefore, the following issues will need to be considered when managing electronic records on the shared network drives:

- Records inventory, file plan and retention schedule; provides a logical and consistent way to arrange electronic records on shared drive. A complete file plan also serves as a records inventory and should include guidance on retention requirements.
- Naming documents and folders, version control, and access control.
- Email management

- Storage and preservation.
- Disposal; due to its technical nature the disposal of electronic records require specific measures to ensure that they are permanently deleted.

SCANNING

Scanning is a process that involves digitally capturing an image of a paper document that is then stored electronically. All service areas undertaking scanning should develop a scanning procedure for their business area.

Scanning requires an investment of resources which will only be worthwhile if the electronic documents can be found and retrieved easily and quickly. This requires documents to be appropriately named within a well-designed folder structure in an electronic document management system or on the shared network drive.

Scanning a large volume of documents can place considerable stress on a shared network drive which may have implications for the performance of the network. Scanned documents are saved as large image files and take up more room than other documents such as spreadsheets and word processed documents. It is advisable to contact Service Birmingham to get advice on ensuring that enough server space is available and an estimate of the likely costs of any additional storage that may be required.

The costs involved in appropriately indexing the scanned images so that they can be retrieved again will also need to be taken into account. If you decide to scan records yourself then this can be a very time consuming and labour intensive process and often a dedicated member of staff is required to carry out this role.

RETENTION OF SCANNED PAPER DOCUMENTS

The decision about how long to retain the original paper version of a document will depend on the reasons for scanning the documents, the quality of the scanning and the legal and regulatory environment in which your service area operates.

Where records have been scanned with the intention of creating an electronic version of the records and the scanning has been undertaken in line with BS10008 Evidential Weight and Legal Admissibility of Electronic Information the electronic version of the record becomes the official record. This means that once the necessary quality checks have taken place the paper version of the record can be destroyed. The electronic record should then be retained for the length of time outlined in the Corporate Retention Schedule.

Where the scanning has been undertaken for retrieval or access reasons and it has been decided that the electronic version of the document will not be the official record, the original paper record remains the official record. The paper version should be assigned the retention date set out in the retention schedule. It can be sent to offsite storage if it is no longer required in the office. The electronic version of the record should not be retained any longer than the period set out in the Corporate Retention Schedule.

Before making a decision to destroy the paper originals it will be necessary to consider the legal and regulatory context of the records. There is no guarantee that scanning in a certain way will ensure that the scanned documents are legally admissible.

If it is anticipated that the scanned records may be required as legal evidence then it is recommended that you obtain legal advice about whether the paper originals can be destroyed, as legal admissibility of the scanned version may depend on the type of document as well as the type of court.

Where it is possible that the records may be required for inspection by any external auditor, regulator or funding body it is advisable to obtain the advice from that external organisation on whether they would accept the electronic copy as evidence. It is advisable to keep a record of the response received as evidence.

RMS has created a guidance document that provides advice on scanning records and includes a risk framework for making a decision about destroying the original paper version of a document. The scanning guideline is available from the RMS pages on Inline.

LEGAL ADMISSIBILITY OF ELECTRONIC RECORDS

Legal admissibility concerns whether a court of law (or other statutory body) will accept a piece of evidence in this case an electronic record. Some evidence may be admitted by the court in a case but the opposing solicitor may call its evidential weight into question. It can be relatively easy to alter an electronic record unlike traditional paper documents, as additions and deletions can be made without the viewer knowing that this has happened. For evidence to be accepted there are requirements on an organisation to prove that the records it creates are; accurate and reliable, have not been altered and are stored in a system that has been secure throughout the record's lifetime. If an organisation is unable to demonstrate this then a record may not be deemed legally admissible and this can potentially harm the case.

There are no firm rules for determining whether an electronic record would be legally admissible but it is possible to maximise the evidential weight of a document by setting up authorised procedures and by being able to demonstrate in court that they have been followed.

HOW CAN I MAXIMISE THE LEGAL ADMISSIBILITY OF ELECTRONIC RECORDS?

There are two standards that electronic information (including scanned images) created and maintained by the Council should conform to in order to maximise its evidential weight. The standards are;

BS 10008:2008 Evidential Weight and Legal Admissibility of Electronic Information specifies the requirements for the implementation of an Electronic Information Management System. This includes specifications on how to capture, store and manage electronic information to increase the likelihood of it being accepted as evidence in court.

BS 10008:2008 Code of Practice for the Implementation of BS 10008 is a set of 'best practice' guidelines, that, if followed will help ensure compliance with BS 10008 and maximise the evidential weight of electronic information.

The main requirements of the standard are to:

- implement an approved information management policy (the relevant Council policies and standards are available on PSPG and Inline)
- agree with external regulators and auditors that electronic working is acceptable
- document your document management procedures and these should conform with the good practice guidance in the Code of Practice
- document your technology systems and configurations
- create and retain adequate and reliable audit trails
- monitor and review the effectiveness of the system managing the electronic information in order to demonstrate its effectiveness.

Following the standard should significantly reduce the risks associated with the admissibility of electronic information. However, compliance with the standard does not guarantee legal admissibility and there will always be an element of risk assessment which service areas will have to undertake and own. The risk assessment will have to take account of; the legal/regulatory environment in which the service area operates and the reputational or financial consequences of the electronic information not being admissible as evidence.

ARCHIVING ELECTRONIC RECORDS

There is currently no archiving software available for departments within the Council to use. A separate archive folder should be created on the shared network drive so that older ‘closed’ records which do not need to be accessed on a regular basis can be transferred to it. The archive folder can be subdivided by year so that the appropriate retention recommendation can be applied to the record type. Records should not be removed from the shared network drive and archived to another storage medium such as DVD or CD as they can deteriorate over time and may become unreadable in the future.

It is recommended that you contact Service Birmingham for further advice on archiving electronic records.

STORAGE AND MAINTENANCE

PAPER ONSITE STORAGE

Records which are still active and in regular use should be retained in filing equipment appropriate for their storage and security and close to where they are used.

OFFSITE STORAGE

Records which need to be retained for legal, regulatory or business reasons but which are no longer in regular use should be sent to offsite storage if space restrictions mean they cannot continue to be accommodated on site.
It is essential that records are sent to offsite storage in a manner that enables them to be located and retrieved effectively in the future. This means that up to date box inventories and indexes of records sent to offsite storage must be maintained.

RMS manages the corporate records management contract for records storage and the current corporate supplier for this service is **Iron Mountain**. No other storage supplier should be used. IMConnect is Iron Mountain’s system which is used for indexing records that are sent offsite and for placing orders for collections and retrievals. RMS delivers free training on the use of the IMConnect system.

If records are stored onsite in Council premises after their active use has ceased, the storage areas should meet the standard specified in the section on storage conditions below. Appropriate records storage is generally not found in attics, basements, portacabins and outbuildings.

STORAGE CONDITIONS

The appropriate temperature for the storage of records is approximately 13-18 degrees centigrade. If the temperature and humidity of the storage area are high this may cause the records to grow mouldy.

Storage areas should be clean, dry and secure. Records should be stored away from potential dangers such as water pipes, direct sunlight and flammable materials.

Records should be stored in suitable storage equipment and off the floor to ensure that they are protected from dust, flooding, pests and rodents.

There should be appropriate access controls in place to keep records safe from unauthorised access, theft and vandalism. Confidential and sensitive information should be stored in equipment and premises that are lockable and secure.

Records should be stored in a way that complies with health and safety requirements. Storage areas should be kept tidy and free from trip hazards. There should be enough room to remove boxes from shelves and open cabinets safely. Boxes should not be overfilled and should be kept to a safe lifting weight.

ELECTRONIC STORAGE

There are cost implications to the Council of storing electronic records unnecessarily. You should avoid storing duplicate copies of documents. The Corporate Retention Policy applies to manual and electronic records.

How and where records are stored electronically will be dependent on the resources and systems available to your service area. Where electronic document and records management systems (such as e-records) or business systems are available for storage of records there should be accompanying comprehensive guidance on which records should be stored in the system and the procedures to be followed.

Electronic records that are not captured into electronic document and records management systems or relevant business systems should be saved to the appropriate shared network areas. Shared network areas should be organised in a way that enables records to be easily located and retrieved.

Information which needs to be retained as a record should not be stored only on portable media such as floppy disks, USB sticks, CDs, DVDs etc. This type of media has an observed life span up to five years caused by material degradation even though published life expectancies are often cited much longer than that. Reliance on hardware and software to read information held and the fact that it is not regularly backed up also makes it unsuitable for medium to long term storage of corporate records. Any records temporarily stored within this media should be tested at least every two years to assure they are still readable.

Advances in technology may mean that software or hardware required to locate, access or use records stored electronically may become obsolete. This should be considered when procuring systems required to capture and manage information, particularly if this information needs to be retained for a period over 10 years.

VITAL RECORDS

Vital records are records which are essential to the continued operation of the Council and those records which are needed to protect the legal and financial rights of the Council and its citizens.

Vital records should be identified and stored in a manner which protects the records from damage or loss. Risk assessments should be undertaken which assess potential threats of loss (this may include fire, flood, vandalism, pest infestation and sabotage). The level and scope of each type of risk should be assessed to determine the level of protection or response that may be required.

Measures for the protection of vital records should be considered as part of business continuity planning. This should include the regular review of records identified as vital and ongoing monitoring of necessary actions and measures in place to ensure that records are protected in a way that is commensurate with the potential consequences of their loss.

ACCESS AND SECURITY

Access to records should be controlled and monitored in accordance with the nature and sensitivity of the records and with regard to relevant legislation. Principle 7 of the Data Protection Act 1998 requires that organisations must take appropriate technical and organisational measures against unauthorised or unlawful process of personal data and against accidental loss or destruction of, or damage to, personal data. Failure to comply with Data Protection legislation could lead to the Council being fined up to £500,000.

Measures put in place should seek to ensure that records are protected from unauthorised access and accidental or deliberate damage. At the same time records should be easy to retrieve and available to those members of staff who are authorised to access them.

Information should be managed in accordance with the Council's Information Security Policies available on the PSPG database.

TRACKING

Tracking procedures are used within record keeping systems to monitor the use and location of records and associated record transactions so that they can be effectively and efficiently retrieved and prevent the risk of accidental mis-filing.

The decision on what information should be captured by the tracking system will be dependent on the type of record and the systems that are used to manage the records.

Where manual tracking systems, such as card indexes or log books, are used there should be clear procedures developed on the use of the tracking system and checks put in place to ensure procedures are followed.

RETENTION AND DISPOSAL

WHICH RECORDS SHOULD BE TRANSFERRED TO ARCHIVES & HERITAGE?

Records that have been identified as having administrative or historical significance should be transferred to Archives & Heritage. The Corporate Retention Schedule provides guidance on which records should be transferred to Archives once they are no longer required operationally. This will be shown in the notes section next to the record type as "Transfer/Offer to Archives". If one of the records in your service area has this note applied to it then you will need to contact the Archives & Heritage team when it has reached the end of its administrative life.

If your department has records which you believe will be of interest to the Archives and Heritage department even though they are not listed in the retention schedule then contact them with details of the records. A decision can be made about whether to transfer them.

Archives Contact Details:
Email: Archives.heritage@birmingham.gov.uk, Tel: 0121 303 4549

HOW LONG SHOULD RECORDS BE KEPT FOR?

The Corporate Retention Schedule is a document that lists the different types of records created and managed by the Council and provides guidance on the length of time each record should be kept. The schedule also outlines the reasons for this retention period and states whether it is a legal or a recommended requirement. Recommendations on retention have to take into account the Council's business needs, legal and regulatory obligations, potential costs and current best practice. RMS work closely with relevant service areas in order to make retention recommendations suitable for the Council's requirements.

The retention periods shown in the Corporate Retention Schedule apply to **all records**, regardless of format.

By following the recommendations contained within the Corporate Retention Schedule the Council can ensure that:

- records are not destroyed when they may be needed for business or legal reasons
- office space and server storage is used effectively by not storing redundant or unnecessary information.

It is also a requirement under the Code of Practice on Managing Records issued under section 46 of the Freedom of Information Act 2000 that an authority should know where all its information is located and how long it should be kept for. Adhering to documented procedures proves that the Council destroys records in the course of business rather than to avoid disclosure.

If you have been set up as a user on the new IMConnect system, you can find the Corporate Retention Schedule under the ‘Policies and Procedures’ section on the yellow navigation bar on the IMConnect home page.

The Corporate Retention schedule is also available via the RMS inline pages http://inline/retention and the PSPG database. If you are unable to find the information you are looking for then contact RMS. We will research the record type that you need the retention information for and add it to the Corporate Retention Schedule at the next update.

SERVICE LEVEL RETENTION SCHEDULES

The Corporate Retention Schedule lists all of the records held by the Council and is therefore a very large document. RMS can work with teams to create department specific retention guidance. The retention guidance is derived from the Corporate Retention Schedule and therefore complies with Council’s Records Management policy. The departmental retention schedule is presented in a clear and concise way, making it easier for staff to find relevant retention procedures for their own team. The document can be designed to include key points on improving information management relevant to the team, helping to improve information management compliance.

For more information about creating a department retention schedule contact RMS.

CONFIDENTIAL DISPOSAL

Once records reach the end of their administrative life, they need to be disposed of in such a way that the information cannot be read or used by other parties.

Efforts must be made to ensure that any information that is destroyed can not be retrieved by reasonable means.

Examples of correct disposal methods:

- Paper records should be shredded preferably using a cross-cutting shredder
- Portable media (memory sticks, CDs, DVDs, floppy disks) should be reformatted, or if this is not possible; bent, scratched or cut into pieces to make them unreadable
- Removal of information from the shared area, personal drives and from any back up devices
- Audio video tapes and fax rolls should be dismantled and shredded
- Destruction of any elements of the record that may have been printed off.

When the information is of a confidential nature the secure destruction is of particular importance. It may be necessary to have the records removed by a specialist contractor to be destroyed in a controlled and secure environment, and in such a way as the level of security associated with the record is taken into account.

Any information on identifiable individuals or commercially sensitive information should be treated as confidential. This needs to be disposed of in a secure manner so that information does not get disclosed to third parties. As mentioned above, it may be necessary to employ a contractor to do this for you. The Council has a corporate confidential shredding contract with **Printwaste** and the company should be contacted to arrange for the confidential waste of any media to be collected. A certificate of disposal will be provided once the records have been securely destroyed. Service Birmingham should be contacted if you have any IT equipment that needs to be disposed of. Until it is collected it should be kept in a secure place.

It is important to remember that if the records are to be destroyed but this has not yet been done and a Freedom of Information request is received for them, then they still need to be made available.

A record cannot be considered to have been completely destroyed until all copies including back-up copies, have been destroyed, as there is a possibility that the data could be recovered. Records held electronically are subject to the same retention periods as paper records. Remember, in the case of electronic records, multiple copies are likely to exist. Ensure that **all** copies are destroyed.

RECORDING THE DISPOSAL PROCESS

Whilst it is not always the case, it is sometimes necessary to make a record of the information that you are destroying. If the information that you are destroying is likely to be needed by a third party or is subject to any audit (internal or external) then it may be necessary to create a record of what you are destroying.

The disposal document should include:

- File reference (or other unique identifier)
- The name of the authorising officer
- File title (or brief description)
- Date when the disposal occurred
- Number of files and date range
- Destruction method
- Confidential destruction reference numbers (if any).

AUTHORITY FOR DISPOSAL

If your records are stored at Iron Mountain you will not need to complete a Disposal Authority document.

When your boxes reach the end of the retention period that was set when they went into storage, RMS will contact you to ask for authorisation to destroy them. You will need to consult the Corporate Retention Schedule to check if the retention guidance has changed since the records went into storage. If no changes have occurred, you will need to confirm to RMS that the box can be destroyed. Iron Mountain will then destroy the records securely and you will be issued with a Disposal Certificate.

If you do not contact RMS within 3 months of the Disposal Review list being sent to you, then we will authorise the destruction of the boxes.

AGILE AND HOMEWORKING

Regardless of your work location, all employees of the Council have an obligation to effectively manage the information they create, use or maintain. All information or data should be systematically managed from creation to destruction to ensure that the Council is able to meet operational needs, legal requirements and community expectations.

Working from home or as an agile worker usually involves storing information on portable devices. Whether staff are working away from a central office or need to share information with other departments portable devices offer an easy way to transport data from one place to another. The fact that portable devices make this process so easy also means they have the potential to jeopardise the security of sensitive or confidential information if they are not managed adequately or are used inappropriately. Portable devices include – laptops, memory sticks/flash drives, PDA’s, CDs/DVDs, ‘Smart’ mobile phones such as a BlackBerry.

There a number of steps that should be taken to ensue the security of the equipment and information that you are using:

- Information on a portable device should be password protected and encrypted.
- Only use a portable device when it is absolutely necessary. This will help us to limit the number of potential security breaches.
- **DO NOT** copy information other than that which you have been authorised to.
- **DO NOT** carry the **only** copy of information with you. A loss of equipment does not have to mean a loss of information.

There are important Council standards relating to information security which you MUST comply with if you work from home or as an agile worker and these are available on the PSPG database.

Remember—whenever you are using a portable device containing Council data, it is **YOUR** responsibility to ensure it is kept safe and secure. Make sure that you are familiar with the standards and guidelines that you must comply with. All equipment and information on portable devices must be securely and appropriately disposed of once their use has ended.

PROJECT WORKING

Project records are those created during the life of a specific project. They can include a variety of information from the planning stage through to completion and post implementation. This information can be in the form of maps, plans, drawings, photographs, diaries, contracts, technical documents, reports, manuals, evaluations and builds an overall picture of the project.

Well maintained records will not only help you to manage the project, but will also help you and others next time. Many projects are repeated or have certain aspects that have been done or researched before and well organised and accessible records allow people to review what has gone before and to benefit from lessons learnt.

RESPONSIBILITIES FOR MANAGING PROJECT RECORDS

The Project Manager is responsible for managing the records that are created during the project and for ensuring that appropriate records management practices are followed including version control, document naming, record retention and disposal.

Where records, such as project records, are created as a result of an activity of a temporary nature the senior manager with responsibility for the activity, usually the Senior Responsible Officer or equivalent is responsible for:

- ensuring appropriate records are created and managed in accordance with records management policy
- ensuring that appropriate resources are assigned to fulfil the responsibility of managing records
- ensuring ownership for the record(s) transfers to the Council once the project has ended

RETENTION OF PROJECT RECORDS

Records retention planning should begin at the start of the project and the list of records and their retention periods should be updated as new documents and record series are created. The Project Manager should be the owner of the records retention plan. If the project is externally funded then reference should be made to the funding authority to determine how long they may require the records to be held for. It may be necessary to contact other organisations or external bodies who require access to the records to determine what their retention requirements are.

Many of the records that are created during the life of a project are common to all projects and retention periods can be determined from legislation or recommendations made in the Corporate Retention Schedule. If you are unable to find a particular record type in the retention schedule then contact RMS.

PARTNERSHIP WORKING

MANAGING PARTNERSHIP RECORDS

The Council has a long history of developing partnerships both within and outside the City as they can be a productive way of achieving a more efficient and effective use of resources. Creating good quality information is essential if it is to be shared between partner organisations.

Records management controls should be applied to the information being shared with or passed to other organisations that the Council is working in partnership with. Particular protection should be given to confidential or personal information.

Protocols should specify when, and under what conditions, information will be shared or passed, and details should be kept of when this information is shared or passed. The Council has a generic ‘Information Sharing Protocol’ (available on PSPG) that applies to information used by the Council (both personal and non-personal data) and relates equally to the use of data and information with partner organisations.

Data Sharing Agreements (DSAs) are the main method for managing the sharing of information between partner organisations as they document the requirements for this to take place. A DSA should be completed for each partnership arrangement that the Council is involved in.

When a partnership is entered into procedures and processes should have already been created to support the work of the partnership and outline the records management requirements. It is good practice to define roles and responsibilities and the boundaries that separate your partnership work from the ongoing operations of each partner organisation so that all parties are clear.

Some of the fundamental issues to be agreed are:

- what information should be contributed and kept and by whom
- the level of information security to be applied
- who should have access to the records
- what disposal arrangements should be in place
- which body holds the information for the purposes of the Freedom of Information Act.

A ‘Partnership Governance Framework and Toolkit’ has been developed by the Council to inform elected members and officers of the standards, processes and rules that need to be followed when working in partnership. The purpose of the toolkit is to help the Council work with its partners to identify if the partnerships they are involved with have good systems of governance.

By adopting good records management practices such as version control, document naming conventions, retention policy and disposing of records in a timely manner it will make it easier for the Council and its partners to demonstrate that they have good systems of governance**.**

WHO IS RESPONSIBLE FOR PARTNERSHIP RECORDS?

Where records are created as a result of partnership working there needs to be clearly defined responsibilities between the Council and the partner organisation for the creation and management of records.

- Where the Council is the lead partner:
  - the Council's records management policy will be applicable
  - the Council will be responsible for the custody and ownership of the records
  - the Council's records management procedures including retention policy will be followed.

- Where another organisation is the lead partner:
  - the records management policy and procedures of the lead partner will be applicable
  - the lead organisation will be responsible for the custody and ownership of records
  - the Council should identify and retain records relating to its role in the partnership required for its own business purposes. They should be retained in line with the Council's Records Management Policy.

- Where there is no identified lead partner the Council should ensure that provisions are made for one of the partners to assume responsibility for the management of the records.

MANAGING EMAILS

MANAGING EMAILS AS RECORDS

A large portion of business activity is recorded within emails. Emails can contain important information that forms part of the knowledge base of the Council and these should be classed as corporate records and managed in line with other business documents.

Emails are disclosable records and can be easily misdirected. It is not a secure medium and should not be used to transmit confidential information or personal data. If your email contains information that is related to work, is the primary source of this information and you can answer 'yes' to any of the following questions, then it is likely to be a record that should be kept.

- Could the email be used to justify or explain a course of action or decision?
- Does the email contain information that will be used as a basis for future decisions?
- Does the email require or authorise an important course of action?
- Does the email approve formal policy or set a precedent?
- Could the email be required to provide evidence of a business activity or transaction?
- Could the email be required as evidence of any liabilities or responsibilities of the Council?
- Does the email protect the rights, assets or other rights of the Council or any of its stakeholders (clients or customers)?
- Does the email the primary source of this information?

It is recommended that you get into the habit of dealing with emails as soon as they are actioned. This will help you to avoid accumulating a large backlog and keep your inbox as clear as possible.

Some email systems save deleted items in another folder rather than actually deleting them. It is important to ensure that emails you meant to delete are actually deleted. The Council's email policy states that email messages should not be retained over 7 years. This element of the policy is now being enforced and Service Birmingham will delete all email messages and related data (e.g. Calendar entries) once they are 7 years old.

If you have a business need to keep email messages for more than seven years, you should save your messages either into an electronic document management system or on your shared network drive. Attachments will also need to be detached and saved to your shared drive.

Emails or attachments that are saved will count against your storage allocations so you should give careful consideration to whether you really do need to keep these messages and/or attachments.

RETENTION OF EMAIL

The importance and therefore the retention period of emails can only be determined by their contents. Different records have different retention requirements. For example an email regarding a variation to a contract will need to be retained for the same period as the original contract. Further guidance can be found by referring to the Corporate Retention Schedule. Not every email needs to be retained - some records contain information that is required only for a limited time to ensure a routine action is completed or a subsequent record is prepared. Such emails should be deleted as soon as they are no longer of use. Examples are:

- copies of reports, newsletters, or information used only for convenience of reference
- correspondence produced for information purposes
- meeting notices and arrangements, cover letters—"please find attached" et cetera
- working drafts that are not required to document the steps in the evolution of a document
- routine enquiries or correspondence.

Some emails can even be destroyed immediately as they do not provide any corporate value. These are:

- internal email messages received as c.c. or b.c.c. messages
- personal emails, jokes, adverts, spam and other unrelated to work emails
- social communications –lunch dates, leaving events, fundraising events, etc.
- general announcements, calendar items and reminders
- email captured threads of later messages.

OUTSOURCING

Outsourcing is the practice of contracting an outside company to provide administrative or operational services that might otherwise be performed by in-house employees. Good records management is a vital for part for the Council's business needs and accountability. Often this task of record keeping could be performed by the staff, but in many cases there are some advantages that come from outsourcing.

REASONS TO OUTSOURCE

There are some circumstances in which it will always be appropriate to outsource:

- Outsource supply usually can provide more flexibility in delivery and costs, and this is particularly useful when the volume of service required is unpredictable.
- Saves money by reducing on-going costs, since the service is provided by the companies who specialise in the field and who have already invested in the necessary equipment and experts, therefore avoiding overhead expenses.
- Enables staff to focus on core functions and chosen priorities which can improve business and management performance.
- There is a need for specialist that the Council could not provide itself, or that it would take too long to develop internally,
- This also means it can improve quality and provide stability, having the details taken care of by outside experts.

KEY THINGS TO CONSIDER

1. Responsibility & Accountability

Even if some records management functions are being outsourced, the responsibility and accountability for all records management issues as well as for having complete and accurate records remains with you as the owner of the records. Regardless of which record management components that are being outsourced, the following responsibilities must be assumed at all times:

- Records ownership
- Security and access control from unauthorised staff and public

It is important to think about responsibilities and accountability requirements when planning outsourcing arrangements. The respective responsibilities of the provider and staff need to be clearly defined and communicated from the start of the outsourcing programme to all staff.

2. Compliance

All records management processes must comply with certain legislations and the Standards and Codes released under it, particularly Data Protection Act and Freedom of Information. This requirement also applies to outsourcing arrangements for any records management activities. As the Council remain responsible for its outsourced activities, it is important to ensure that contractors are aware of their responsibilities under the Act and manage their records accordingly.

The best way to meet these 2 requirements is to ensure the following:

- Select a reputable organisation offering suitable guarantees about their ability to ensure the security of personal data.
- Make sure the organisation has appropriate security measure in place and appropriate checks on their staff.
- The contract makes specific provision for recordkeeping requirements and compliance measures.
- The contract should also requires the organisation to report any security breaches or other problems, and have procedures in place to allow you to act appropriately.

Selection process for the chosen outsourcer normally is undertaken by the Corporate Procurement Service, who then provides a list of approved suppliers accessible from Voyager. Any outsourcing arrangements must be in accordance with the Birmingham City Council's Procurement Framework. Remember records are part of the corporate assets and they are required to support Council's business and accountability requirements now and in the future.

OUTSOURCING RECORDS MANAGEMENT FUNCTION

Records management consists of different functions. The best way of looking at how outsourcing can give the greatest benefit to which records management function is to use the concept of the 'life cycle of records'.

There are four phases to the life cycle of records (Creation / Receipt → Active → Inactive → Final Disposition); examples of type of activities that can be outsourced with their benefits explained on the following table.

Examples of outsourcing records management functions with their benefits:

Records Life-Cycle	Examples of activity	Benefits	Considerations
1. Creation / Receipt	Data entry	- Enable staff to focus on core functions - Improvement on data quality	- Confidential and sensitive information must be processed in a secure manner. - Can limit level of understanding of data own due to processed by external
2. Active (high value and use), and 3. Inactive Records (lower value and use)	File plan*	- Supports accountability and good governance - Having specialist / expert work - Compliance with legislations	Bespoke training on how to use and do maintenance
	Retention schedule development*		
	Filing / storage	- Potential space saving leads to potential cost saving - Security compliance	Contract management with outsourcer
	Scanning & indexing**	- Easy access of files - Cost of office space saving	- Cost of process and maintenance - Legal admissibility
4. Final Disposition	Shredding / confidential waste	Compliance with legislations	Control to ensure destruction only take place by staff authorisation

* Records Management Service can offers its expertise on developing file plan and departmental retention schedule specific to team's records free of charge

** Birmingham City Council has a specialist in-house team that provides the scanning service

RECORDS MANAGEMENT SERVICE

The Records Management Procedures Manual has been developed by RMS. If you require further guidance on any of the information contained within the manual or any other aspect of records management then please contact the RMS team on:
records.management@birmingham.gov.uk