



**A CONCISE REFERENCE GUIDE TO THE
MANAGEMENT OF ELECTRONIC DOCUMENTS**

RELEASE 2 (Version 19)

8th October 2006

TABLE OF CONTENTS

1	Executive Summary	3
1.1	Scope and Limitations of this Document	3
2	Introduction	4
3	Clarification of Terms	5
3.1	Definitions	5
3.2	Common confusion between backups and archiving	5
3.3	E-mail archiving	6
4	Effective Information Management	7
4.1	The need to keep records	7
4.2	The need for effective document retention and destruction policies	7
4.3	Electronic document management and records management	8
4.4	Spam	9
4.5	Effective Access Controls	10
5	Compliance with the Law Society's guidelines	11
5.1	Solicitors' Practice Rules 1990	11
5.2	Law Society Guidelines – printing of e-mails	11
5.3	Guidance on electronic storage systems	12
6	Employee Issues	12
6.1	Responsibility for e-mail and document management	12
6.2	Internal control and corporate governance	13
7	Undertakings provided by law firms in respect of the destruction of documents	14
8	Evidential issues relating to electronic documents	15
8.1	Electronic documents as evidence in civil proceedings	15
8.2	Electronic disclosure	15
8.3	Ability to retrieve e-mails	16
8.4	Code of practice for legal admissibility and evidential weight of information stored electronically – BIP 0008 (www.bsonline.bsi-global.com)	17
8.5	Code of practice for electronic documents and e-business transactions for evidence, audit and long-term duty of care – PD 5000 part 2	18
8.6	Information security management – British Standard 7799	18
8.7	Guidance	19
9	Data Protection Act 1998	19
10	Copyright	20
11	Guidance on statutory and regulatory retention periods	20
12	Best Practice Guidelines	22
12.1	International Standards Organisation (www.iso.org)	22
12.2	The Model Requirements for the Management of Electronic Records Specification	22
12.3	The National Archives Functional Requirements for Electronic Records Management Systems (ERMS)	23
12.4	Butler Group report on e-mail management (www.butlergroup.com)	23
12.5	ARMA	24
12.6	The Sedona Guidelines: Best practice guidelines & commentary for managing information & records in the electronic age	24
12.7	The Commercial Litigators' Forum: Electronic Disclosure (27 October 2004) ..	24
13	Emerging industry best practice regarding electronic document management and retention	25
13.1	Industry best practices	25
13.2	Proposed model	26
13.2.1	Old data	29
14	Acknowledgements	31
15	Document Control	32

1 Executive Summary

As the traditional paper based way of conducting business is becoming less common, businesses are now reliant on the use of e-mail and electronic means of creating and storing documents. Along with the benefits of such technology comes exposure to new risks. Law firms and their clients must contend with an increasing raft of legislation and regulations and ensure compliance. As well as remaining compliant, managing partners and IT directors must also make sure their document management systems meet their firm's operational requirements. It is, therefore, vital that law firms are aware of the need for a fully integrated information management policy. This guide addresses the main issues to take into account when implementing or updating an information management strategy involving the management, retention and disposal of electronic documents including:

- consideration of the Law Society's publication of its revised 2005 E-mail Guidelines for Solicitors which provides advice as to good practice in relation to e-mail use. In particular, the Guidelines clarify that it is not necessary for law firms to print e-mails if these are held in a suitably managed electronic storage system;
- explanation of the importance of having a comprehensive electronic archiving system in place rather than continuing to rely on backup tapes to retrieve electronic information, as access to such tapes is generally problematic;
- advice as to the main legislative, regulatory and evidential issues affecting the use of electronic document management systems, such as obligations imposed by the Data Protection Act 1998, retention periods for different categories of documents, disclosure of electronic documents in civil proceedings and copyright issues when storing information in such a system, and
- inclusion of a number of best practice standards as practical assistance for law firms, together with references to sources of further information.

Whilst this guide addresses many areas where effective processes, controls, tools and technology can be put in place, often a change in culture is required within a firm to give the issue of information management sufficient weight and for each individual in the firm to understand that it is their responsibility to manage the firm's information. Staff must be encouraged and supported by senior management to follow the procedures and use the technology correctly and consistently in line with the firm's policies. The combination of culture, policies, processes and technology, when combined correctly and managed effectively, can deliver exceptional results that can lead to reduced risk, lower claims, greater efficiency and reduced costs of information management.

1.1 *Scope and Limitations of this Document*

This document has been produced with consideration primarily of UK legislation and the guidelines produced by the Law Society of England and Wales and does not fully take into account legislation outside of this jurisdiction.

In addition, this document has been compiled with commercial SME (small and medium enterprise) and large law firms in mind and so the technology solutions discussed may be less applicable to very small partnerships or sole practitioner firms.

Legislation and guidelines change frequently and this document is considered a sound reference guide based on those guidelines and legislation published up to the full release of this document on 8th October 2006.

2 Introduction

With more efficient ways of communicating, and technology developing at an ever faster rate, the traditional paper based way of conducting business is in sharp decline. It is now normal practice for the vast majority of organisations to use e-mail extensively and send documents electronically. As well as e-mail, other electronic means of communication are being used including instant messaging, voice-mail, mobile telephones, digital dictation and video recordings. The various means of communication that we now use indicate that the concept of a pure paper file containing all relevant matter related material is becoming a thing of the past. Despite this, many people continue to treat electronic communications, such as e-mail, as an informal extension of an oral discussion and some organisations erroneously view e-mail as an entirely transient means of communication. With the widespread use of technology such views could have costly consequences for law firms and their clients given that electronic communication, just as paper, is subject to legislative, regulatory and judicial control. Law firms and their clients should, therefore, ensure that their information management strategy, including their document management, retention and disposal policies, extend to all documents, including e-mails, that are created and stored electronically.

There is a tendency to shift some, if not all, of the responsibility for the electronic storage of documents and file management to the IT department. IT departments, however, are not responsible for creating or justifying a law firm's information management strategy. It is the management of the firm's responsibility to deal with this issue, not the IT department. Information management is a business, not an IT, issue. The IT department is merely the custodian of the electronic record, not the controller.

Effective information management involves implementing a number of processes, applications and tools to support the firm's document production, retention and e-mail systems. It also creates a level of control that is necessary to ensure the firm complies with the relevant regulations and legislation to which law firms and their clients are subject to.

In addition to effective processes, controls, tools and technology being put in place, often a change in culture is required within a firm to give the issue of information management sufficient weight and for each individual within the firm to understand that it is their responsibility to manage the firm's information. Staff must be encouraged and supported by senior management to follow the procedures and use the technology correctly and consistently in line with the firm's policies. The combination of culture, policies, processes and technology, when combined correctly and managed effectively, can deliver exceptional results that can lead to reduced risk, lower claims, greater efficiency and reduced costs of information management.

This guide cannot and should not explain to managing partners and IT Directors how to change the culture in their firm. It is designed, however, to address the main issues when formulating or reviewing a comprehensive information management strategy that involves the management, retention and disposal of electronic documents. The guide addresses a number of significant issues including:

- the important differences between backing up data, archiving data and the integrity of the data;
- retention and destruction policies;
- legislation, regulation and compliance obligations (especially in respect of the Law Society of England & Wales), and
- best practice guidance.

There are many legislation and compliance related issues affecting the management of electronic documents and also a range of best practice guidance from several bodies. The aim of this guide is to summarise the most pertinent issues and produce a concise reference guide with pointers to other relevant sources should the reader wish to obtain more detailed information.

3 Clarification of Terms

3.1 Definitions

It is important to differentiate between some of the more important terms used in this document before continuing to read it.

Archive – This is an organised, logical and deliberate collection of records designed for future reference and keeping a record of a document in a particular state of its evolution or development (for example – a version, or a state at a particular date). An archive will be retained for a specified period, whether for regulatory or other business reasons. The date on which records are moved to an archive and possibly then subsequently destroyed will be determined by the organisations' policies, the criteria attached to the file/matter to which the data belongs and legislation. Each individual record and set of records in an archive should be tagged with relevant metadata to allow the data to be searched for and recovered as necessary. Archives may be supported by an electronic records management system and different storage media and, if so, should be backed up.

Backup – This is a snapshot of data at a fixed point in time, recorded for the purpose of disaster recovery. It is designed for database, system or server wide recovery following the failure, corruption or loss of a system. As such, the granularity of backups is often at an “all or nothing” level. Snapshots are taken at intervals defined by the criticality of the need to keep the data up-to-date, and are retained for periods considered necessary to recover to a point in time that is likely to be required.

Electronic document management – This is an electronic system that allows an organisation and its users to create a document or capture a hard copy in electronic form and store, edit, print, process and otherwise manage documents in image, video and audio, as well as text form. An electronic document management system may include scanners for document capture, printers for creating hard copy documents, storage devices, and computer servers and server programmes for managing the databases that contain the documents.

Electronic document retention – This is an electronic process to control the distribution, storage, review and disposal of electronic information created, received and maintained as evidence and electronic information created and stored by an organisation or person in pursuance of legal obligations or in the transaction of business.

Forensics – This term indicates the recognition that data, from the moment it is created or received, if subject to appropriate techniques to protect its integrity, is likely to be considered forensically acceptable in a court of law.

Integrity – This term is used, in terms of data and network security, as an assurance of the authenticity and evidential weight of data. The degree of assurance depends on the measures used to ensure the integrity of the data, including the control mechanisms in place in relation to the physical environment and how access to data is restricted.

Metadata – This is information relating to a record that is not the record content itself (it is in effect, data about data). For example, an e-mail has hidden data about its mail route, the encoding used, the technical system identities of the sender and recipient and their respective system, servers and networks. This is one example of metadata. Often, however, the e-mail content (the body of the e-mail) is regarded as the *record*, and in this case the data such as sender name, recipient name, subject title are often referred to as metadata.

Record – This is a document or other piece of data that has been 'declared' as requiring retention to act as an account of occurrence or evidence of being (often but not solely relating to a client/matter/internal file or audit trail.) Declaring a record is the act (whether automated, rules based or user initiated) of flagging a document or other piece of data as being a record.

3.2 Common confusion between backups and archiving

The practice of keeping backups for a long period of time has developed to enable a firm to recover from a problem that is discovered long after the event (for example a data corruption).

Often, year-end backups are kept indefinitely. This leads to confusion and the belief that backups are an effective archive. They are not.

Backups are usually mistaken for archives by business users rather than IT departments but sometimes both business users and IT departments use the terms interchangeably. IT departments are frequently asked to recover an e-mail relating to a client-matter or provide records from backups to satisfy a subject access request under the Data Protection Act 1998. The former should have been a matter for policy and archiving, the latter is one for forensics (i.e. proving whether something happened, or not). Recovering records from backups is cumbersome, time consuming, unreliable and inaccurate. For example, often a whole e-mail system must be restored to extract a single e-mail from one person's mail box, and if an e-mail was received and deleted before a backup cycle began, it will not be held in backup. Where a separate archiving system records the e-mail, the possibility of a user deleting the e-mail is reduced significantly.

It should also be noted that, in order to comply with the requirements set down by the Data Protection Act 1998 (see section 9 below), backups should not be kept for longer than necessary if they contain personal data. It is, therefore, necessary to review the content of backups on a regular basis.

Therefore, firms should:

1. ensure that data with differing retention requirements are separated in systems as much as is practical / cost effective in order to prevent backup and long term storage of data that should be deleted and expunged for regulatory purposes (for example separating Finance and HR data), and
2. retain backups only for so long as is necessary for system recovery purposes. Once adequate and properly managed archival systems are in place backups should never be required for recovery of records. Care should be taken, however, as access to data created prior to the establishment of adequate and properly managed archival systems may only exist on current backups so recovery may be compromised if all backups are destroyed.

3.3 E-mail archiving

E-mail archiving is now commonplace and constitutes the organised storage of records for future reference. E-mail archiving differs from the true definition of archiving because it is generally system driven (although it can be user driven) and is designed to reduce the amount of stored documents in an e-mail system. The main purpose is to maintain system performance and to reduce the size of backups so as to speed system wide recovery and restore from backups in the event of loss of e-mail service. As such, e-mail archiving is a software tool which ensures e-mail system efficiency and disaster recovery rather than being a record keeping or true archiving system.

The fact that e-mail archiving systems have, over time, added functionality, search criteria and other tools has meant that such systems are considered by users to be an effective archiving tool. E-mail archiving, however, is not true archiving and suffers the following problems:

- without logical, formal structure and additional metadata it does not present such a reliable retrieval method as a client-matter referenced archive;
- it only stores e-mails and attachments, which in effect creates more than one storage location for client-matter files, given that matter related documents will be stored elsewhere, and
- the filing period in automatic e-mail archiving tools is driven by a set time period or the size of the user's e-mails or mail box and so does not correspond with record management principles designed to capture records at a certain state in time or in the evolution/development.

Firms should, therefore, ensure that a system is in place for the true archiving of e-mails which stores the e-mails in the correct electronic client-matter file.

Some useful guidance on selecting e-mail archiving systems is available in Appendix 4 of Stephen Mason's book *E-mail, networks and the internet: A concise guide to compliance with the law* (xpl publications, 6th edn, 2006) ISBN 1 85811 3563

4 Effective Information Management

4.1 The need to keep records

The reason why a particular record needs to be kept will affect how long it should be retained. The consequences of managing information and records inadequately in the electronic age include:

- inability to retrieve and use business critical information on a daily or historic basis;
- increased costs of conducting business due to disparate or inaccessible data;
- possible breaches of statutory or regulatory retention requirements, and
- reduced ability to comply with court orders or other litigation related obligations requiring access to existing information.

The main reasons to retain records are:

- to comply with statutory and regulatory requirements, for example, anti-money laundering and market abuse regulations requiring the retention and tracking of particular documentation: in these cases compliance is not optional;
- for audit purposes: these may dictate that records need to be kept until a statutory or contractual audit has been completed;
- for evidential requirements: the risk of potential litigation and issues relating to the admissibility and the evidential weight of documentation will affect how electronic, as well as paper documents, are retained as well as the duration of their retention;
- some documents should never be destroyed: these include current documents of title, share certificates and property deeds; and
- business or commercial reasons, for example, keeping documents for know-how resources: however, the above categories should always take precedence to this category.

4.2 The need for effective document retention and destruction policies

Given the consequences of failing to manage information, law firms and their clients should have a document retention policy in place which:

- sets out document security classifications and access restrictions;
- identifies which documents and records should be retained, and the minimum retention periods for each type with reference to relevant legal and regulatory provisions;
- identifies procedures for selecting records for retention or disposal, and the frequency with which that selection process should take place;
- after a careful assessment of the risks, minimises the retention of other records while ensuring that the information requirements of the firm are met;
- retains records in a manner appropriate to their purpose throughout their life and specifically:
 - ensures that records which may need to be tendered as evidence in legal proceedings are kept in a manner that ensures that they will be admissible in court and given full weight; and

- ensures that records kept for regulatory purposes are kept in a manner suitable for those purposes;
- reflects the way in which documents are created and altered to comply with record keeping requirements;
- specifies procedures for the disposal of records;
- disposes of records that are no longer needed in an efficient, orderly and appropriate manner and ensures that all disposal actions are properly recorded;
- allocates clear responsibility for the implementation of the policy, and
- sets out training and education processes to ensure awareness of, compliance with and the ability to use the systems in place to manage the above.

Firms should record the rationale and approval process behind the policies as defence should the policies be questioned in the future, and audits of compliance with the policy in the firm together with records of the audits and results should be kept. This will strengthen the commitment within the firm whilst at the same time acting as strong defence should the firm be questioned on its policy and management.

The Australian first instance case of *Rolah Ann McCabe v British American Tobacco Australia Services Ltd [2002] VSC 73* illustrates the need for organisations to have proper policies in place in order to avoid adverse inferences being made during civil litigation. The judge held that British American Tobacco's defence should be struck out because he considered that the company's document management policy was merely a cover for the deliberate destruction of documents relevant to Mrs McCabe's claim. He stated that "*the primary purpose for the reduction of documents was to impede the prospects of success of any plaintiff who brought proceedings against the Defendant.*"

Although this decision was overturned on appeal, with the court recognising a legitimate commercial need for companies to limit the scale of retained documents, the case acts as a warning that document retention and destruction policies are likely to be subject to scrutiny in the future. Firms should ensure that they are able to justify such policies as reasonable, measured and appropriate. As electronic data occupies less space and can be cheaper to store, it should be questioned whether it is justifiable to destroy electronic material on the same time scale as paper files. It is, therefore, arguable that a court is more likely to draw adverse inferences from the lack of proper management of electronic documents, such as failing to transfer business e-mails from a user's e-mail inbox to the relevant client or matter file, or their deletion from a user's inbox altogether, if this results in relevant information failing to be disclosed.

4.3 Electronic document management and records management

The differences between electronic document management and electronic records management lie in the objectives that each solution satisfies.

Requirements for electronic document management

Electronic document management exists to support immediate operational requirements for business information but does not generally address the need to retain and dispose of that information. Electronic document management helps law firms and their clients exploit their information by enabling employees to obtain access to and share information, therefore reducing storage costs and helping to address any immediate and future risk considerations. Typically, electronic document management systems will capture information produced in both electronic and paper form and will provide for:

- storage and indexing at the document level;
- search and retrieval at the document level;
- access management and security control;

- off-line archiving of semi-active or inactive documents;
- version control;
- audit trails on access and changes to the document;
- document profiles, and
- integration with document image processing and workflow systems.

Requirements for electronic records management

Electronic records management meets additional needs. It provides an environment for capturing electronic documents and applying standard records management practices, based on an approved disposition and review schedule, and generally supports the medium to long-term requirements of the firm. As well as meeting the needs of electronic document management, electronic records management supports:

- capturing, storing, indexing and retrieving all elements of the record as a complex unit, and for all types of record;
- management of records within class categories or filing structures to maintain the narrative link between records;
- recording metadata describing contextual information;
- integration between electronic and paper records;
- secure storage and management to ensure authenticity and accountability, including support for legal and regulatory requirements;
- appraisal and selection of records;
- systematic retention and disposition of records, and
- migration and export of records for permanent preservation.

An effective electronic records management system will preserve the content, structure and context of the electronic records, ensure that documents which are kept as records are “registered”, and that authentication procedures and audit trails are put in place to provide for the integrity of the data. This will help provide for the weight of the evidence, improve corporate accountability and assist law firms and their clients in meeting the requirements of internal and external auditors.

The recent fires at two Iron Mountain facilities have prompted more law firms to expedite their timetables to move to electronic document and records management.

The fire at Iron Mountain’s London facility destroyed documents belonging to several law firms including Allen & Overy LLP, Norton Rose and Simmons & Simmons. The impact of the fire was felt least by firms which already had electronic information management systems in place and had stored the majority of client-matter related documents electronically, minimising the volume of client-matter related information retained in paper form and stored at off-site facilities. Firms which did not have such technology in place are now expediting their implementation of such solutions.

4.4 Spam

It is estimated, not without justification, that nearly 70 per cent of the world’s e-mail is spam. Ideally, spam e-mails should be filtered out, either by a third party outside the firewall or by the firm itself inside the firewall. The former solution risks the loss of important business e-mails as they are filtered out. However, where spam is not filtered, the firms must then decide

what to do with e-mails identified as spam. It can be difficult to distinguish between business e-mails that need to be retained and e-mails that can safely be deleted as spam, particularly when a regulator needs to be satisfied that business e-mails are not being deleted with the spam. There are three different approaches to this problem:

- retain all e-mails, including the spam. The drawback of this is the size of the archive and the effect on searching the archive;
- filter out non-relevant e-mails, possibly by using an external spam filter, with the ability to check rejected e-mails to ensure that they are only spam, or
- keep all e-mails but categorise them according to content and give different retention periods to each category, giving spam e-mails a short retention period.

Several law firms are now taking the approach of quarantining blocked e-mails and either allowing employees to check, or appointing an administrator to decide, which are genuine e-mails. This process will, of course, have to be supported by sufficient training and working practices.

If economically viable, it is recommended that non-relevant e-mails are filtered out using a spam filter managed outside the firm's firewall. If such a system is adopted, periodic notifications should be sent to all intended recipients which provide summaries of the e-mails which have been filtered out, with each recipient being responsible and under policy for checking that no business related e-mails were caught by the filter. This responsibility should be included in the firm's information management policy and guidelines. The verification of such spam notifications should not be delegated to an administrator uninvolved in the client-matter (for example, in the IT or Facilities departments). Verification requires working business knowledge to ensure that any legitimate business e-mails caught by the filter are correctly identified and retrieved. It may, however, also be prudent to adopt a policy which requires any non delivery of business related e-mails to be reported to a central body within the firm so that the parameters of the filter can be reviewed and adjusted from time if necessary. As a further measure, recipients of e-mails should be trained to "white-list" any contacts from whom business e-mails were rejected by the spam filter to ensure that future genuine e-mails are delivered, as well as personally "black-list" any spam e-mails not caught by the filter. Whitelisting is particularly important when dealing with clients whose business may be prone to triggering anti spam or access control software.

Due to the risk of filtering out legitimate business e-mails when using spam filters, it is recommended that firms notify clients in their standard terms of engagement of the use of a spam filter and the possibility that not all e-mails sent to the firm will be received. Section 5.3 of the Law Society's E-mail Guidelines for Solicitors (November 2005) recommends that clients should be asked to follow up important e-mail communications by phone, fax or a printed copy sent by post.

A method of recording all e-mails that arrive within or depart from the firm, either by using a forensics system or journaling in e-mail systems should be considered to enable firms to prove non-delivery. Firms using anti-spam tools (particularly outsourced tools) should understand the retention period of spam records, as past this timeframe it will not be possible to explore non-delivery of an e-mail.

4.5 Effective Access Controls

Providing adequate and properly managed records management and archive and retrieval systems provides users with greater ability to recover files but also provides for easier unauthorised access unless policies and systems are in place to control access and destruction requests.

As systems move to be more electronic, access is widened and firms should pay particular attention to ensuring adequate physical and electronic access controls, procedures, policies and audit checks are in place to secure records and data held. External testing of the security of such systems is recommended especially where firms deal with particularly sensitive personal or commercial information.

5 Compliance with the Law Society's guidelines

5.1 Solicitors' Practice Rules 1990

Rule 1 (Basic Principles) of the Law Society's Solicitors' Best Practice Rules 1990 (**Practice Rules**) states:

"A solicitor shall not do anything in the course of practising as a solicitor....which compromises or impairsthe solicitor's proper standard of work"

It is widely accepted that failure to keep full and accurate records of a client matter would be a breach of this requirement. This rule is likely to be breached if record keeping is such that some documents are stored in a paper file, others in an electronic document management system and further documents in an e-mail system without correct and sufficient referencing to all the related documents to constitute a complete client-matter file. This is especially true if access to a file is limited (for example, personal e-mail folders) or proper care is not taken as to the security of documents or archiving of material for appropriate periods of time.

Rule 13 (Supervision and management of a practice) of the Practice Rules states that:

"(1) The principals in a practice must ensure that their practice is supervised and managed so as to provide for:

- (a) compliance with principal solicitors' duties at law and in conduct to exercise proper supervision over their admitted and unadmitted staff;*
- (b) adequate supervision and direction of clients' matters;...*
- (d) effective management of the practice generally."*

It can be argued that the inability of a firm to produce a complete and accurate client-matter file could be in breach of rule 13 as it makes supervision of the file more difficult and less effective. Re-constitution of a complete and accurate client-matter file becomes increasingly difficult in large firms with many lawyers working on a matter across offices. Information management becomes increasingly important (and unfortunately more complex) in geographically dispersed teams.

Sections 2.2, 3.3 and 3.4 of the Law Society's E-mail Guidelines for Solicitors (November 2005) recommends that firms should have a written e-mail policy in place to ensure compliance with this practice rule. All staff should be made aware of such a policy and it should be enforced.

5.2 Law Society Guidelines – printing of e-mails

Previous versions of the The Law Society's E-mail Guidelines for Solicitors (2004 version) stated:

*"3.18 Firms should take a pragmatic and common sense approach to records of e-mails. That is, significant and substantive e-mails (including e-mails that are subject to statutory retention periods) **should be printed and stored**, but those that are ephemeral can be left to expire from electronic storage in the ordinary course of events."*[emphasis added]

Many law firms misinterpreted this guidance as a regulatory requirement or practice rule that they had to adhere to. Given this, lawyers often print out e-mails and keep them on file (if, of course, they have not already been deleted) on the incorrect assumption that the paper version of the e-mail is the most accurate, permanent record, given the ease with which electronically held documents can be altered. Printed versions of e-mails and documents are, however, of little value given that the metadata is not retained. In many cases, the most accurate evidence will be the electronic version of the e-mail or document, provided that the

firm has suitable software that verifies the integrity of the document. The electronic record should retain two main types of information:

- the content of the document and its internal structure, and
- the metadata, which describes the record and each of the constituent parts, including the routing of an e-mail.

Additionally, it is more economic for firms to operate on a less paper intensive basis, as this has cost, space and time saving benefits. In recognition of this, the Law Society published revised E-mail Guidelines for Solicitors in September 2005, which provide firms with the following advice:

*“3.18 Firms should take a pragmatic and risk-based approach to records of e-mails. This is, significant and substantive e-mails (including e-mails that are subject to statutory retention periods) **should be stored in a suitably managed electronic storage system or printed and stored**, but those that are ephemeral can be left to expire from electronic storage in the ordinary course of events.”* [emphasis added]

The more recent revision of the Guidelines (November 2005) retains this important ability to file e-mails in a suitably managed electronic storage system.

On this basis, **it is not necessary for lawyers to print out and store in paper form** all matter related information provided that it is retained in a “suitably managed electronic storage system”. It is recommended that such a system should constitute a complete client-matter file.

5.3 Guidance on electronic storage systems

Although the Law Society has not issued specific guidance as to what constitutes a “suitably managed electronic storage system”, Litig’s view is that, as well as adopting the best practices outlined in section 13 of this paper, law firms must, as a minimum, ensure that their electronic document management system:

- forms part of an extensive business continuity and disaster recovery plan;
- has the ability to store different types of information including documents and e-mails;
- is fully auditable both at the operating system level and the application level;
- has suitable internal and external security and access control processes (including adequate encryption technology if the system is client facing);
- is linked to a comprehensive backup process and an archiving or document retention solution, and
- is fully supported by internal working practices (including those covering risk management) which in themselves are driven by the firm’s written policy, ensuring that the technology is used in the most effective manner.

6 Employee Issues

6.1 Responsibility for e-mail and document management

Effective information management involves making sure that employees are trained and aware of the retention obligations, as well as making sure that they do not send contentious e-mails, internally or externally, that could subject the firm to litigation or exposure in the press. It cannot be assumed, for example, that employees realise the implications of sending personal e-mails if they have never been informed of the consequences.

The employment dispute *Sangster v Lehman Brothers Ltd* heard at the London Central Employment Tribunal in October 2002 (Case No. 2201857/2002) highlights the potential pitfalls for employers. Mr Sangster, an employee of Lehman Brothers, sent an offensive e-mail

to a colleague, as a result of which he was dismissed. Mr Sangster sued his employer for wrongful dismissal and breach of contract. The employment tribunal held, on appeal, that although commonsense should have warned Mr Sangster that sending the offensive e-mail was unacceptable, Lehman Brothers had failed to provide its employees with proper training as to the content of the company's technology policy and, accordingly, the sanctions for sending inappropriate e-mails. It was also held that the technology policy was not enforced consistently and the disciplinary process was flawed. As a result, Lehman Brothers was held 50 per cent liable for breach of Mr Sangster's employment contract and wrongful dismissal.

(Source : *E-mail, networks and the internet: A concise guide to compliance with the law* (xpl publications, 6th edn, 2006) ISBN 1 85811 3563)

It is vital, therefore, that firms follow the Law Society's advice in the updated 2005 E-mail Guidelines for Solicitors:

"3.4 A written e-mail policy should be brought to the attention of all partners, consultants and staff (temporary and permanent) and it should be enforced. It should be reviewed regularly and it should link to other relevant policies (for example, equal opportunities or IT security policies)."

As a minimum, the following issues should be brought to the attention of the employee:

- possible breach of confidentiality when using e-mail; it should be considered how much information should be transferred by e-mail. The Law Society advises that the use of encrypted e-mail should be considered, particularly where personal data, which is required to be secured under the Data Protection Act 1998, is included in an e-mail;
- the types of information that employees can and cannot transmit;
- retention periods should be observed in relation to record keeping requirements for e-mails as well as other documents;
- the length of time communications are retained; employees should not be misled into believing that e-mails are deleted if they remain stored on the firm's servers or back-up tapes;
- restriction on the personal use of e-mail and internet to avoid losing productive time;
- risk of viruses through the use of unauthorised software, and
- sanctions for failing to comply with the policy.

6.2 Internal control and corporate governance

The report, *Internal Control: Guidance for Directors on the Combined Code* prepared by the Internal Control Working Party, chaired by Nigel Turnbull and published in September 1999, provides advice to listed companies on internal controls to safeguard shareholders' investments and the company's assets. The report outlines the elements of a sound system of internal control as encompassing:

"the policies, processes, tasks, behaviours and other aspects of a company that, taken together:

- facilitate its effective and efficient operation by enabling it to respond appropriately to significant business, operational, financial, compliance and other risks to achieving the company's objectives. This includes the safeguarding of assets from inappropriate use or from loss and fraud, and ensuring that liabilities are identified and managed;
- help ensure the quality of internal and external reporting. This requires the maintenance of proper records and processes that generate a flow of timely, relevant and reliable information from within and outside the organisation;
- help ensure compliance with applicable laws and regulations, and also with internal policies with respect to the conduct of business."

The report provides concise guidance which can be used by law firms as a basis to advise their blue-chip clients on electronic document management issues within the scope of corporate governance. By including a communications system and guidance policy, a company will be seen to recognise that certain risks exist and demonstrate that it is actively monitoring the exposure it faces when using networked communications in the workplace. Although not directed at partnerships, the report outlines principles which can be applied equally to law firms when reviewing their internal control policies. The full report can be found at http://www.icaew.co.uk/viewer/index.cfm?AUB=TB2I_6342

7 Undertakings provided by law firms in respect of the destruction of documents

Clients of law firms are often required to give undertakings as part of, or separate to, a confidentiality agreement to return or destroy information relating to a proposed transaction. In almost all cases, the client is required to bind all persons who have received the information, and are acting on their behalf, to the same obligation. This includes the law firm advising the client, requiring the law firm to destroy matter related information. This occurs regularly in transactions relating to the proposed sale of a target company where the seller provides the potential purchaser(s) with information relating to the target company and its affairs (**Information**). A restrictive undertaking in such a transaction may read:

“If the purchaser ceases to be interested in the proposed transaction and in any event upon the written request of the seller, the purchaser will immediately at its own cost and expense:

- (a) return to the seller (without keeping any copies) all documents containing Information or relating to the negotiations or discussions about the proposed transaction (whether or not in the possession of the purchaser);
- (b) expunge all Information from any computer, word processor or other device containing the Information and belonging to the purchaser, its authorised recipients or any other person in which it is held, and
- (c) if so requested by the seller, the purchaser shall deliver to the seller a certificate signed by the purchaser’s company secretary or other authorised officer confirming that the obligations contained in this paragraph have been complied with.”

Such an undertaking cannot actually be fulfilled by the law firm (or their client) because:

- the return or deletion of matter related information by a law firm will be in breach of its regulatory obligations to retain all matter related information for a specified period; and
- deletion of information held electronically is extremely difficult and onerous. It is probable that a number of copies of an e-mail or electronically stored document will exist, for example, in the sender’s and recipients’ mailboxes, on multiple backup tapes and on hard drives. Additionally, there are fundamental differences between merely deleting a document and actually deleting and expunging it.

To address these issues, such undertakings must have two crucial caveats:

- the first should carve out an exception to returning or deleting documents where they are required to be retained by law or regulation or by competent judicial, governmental, supervisory or regulatory bodies, and
- the second should carve out an exception to returning or deleting documents where it is not practicable to do so, or specifically exclude from the undertaking the deletion from automated back-up systems, which are not readily accessible by anyone other than the provider of the undertaking.

8 Evidential issues relating to electronic documents

8.1 Electronic documents as evidence in civil proceedings

Rule 31.4 of the Civil Procedure Rules 1998 (CPR) defines a document as “anything in which information of any description is recorded” and so includes any electronically held data.

The Civil Evidence Act 1995 (CEA) resolved many of the problems of legal admissibility that arose from documents being generated by or held on computers. The CEA shifted the argument away from whether such documents would be admissible in civil proceedings to the evidential weight of a document. Under the CPR, a party is deemed to admit the authenticity of a document disclosed to him unless notice is served that he wishes the document to be proved at trial. To ensure the evidential weight of documents is not compromised, law firms should advise their clients to:

- ensure that software is in place which can authenticate electronic documents;
- preserve the electronic records as to the composition of a document which details the document creation date, author, dates when changes have been made, date and time the document was sent to a particular recipient, and
- ensure that audit trails exist which demonstrates that a particular document was sent as an attachment to an e-mail.

The CEA no longer contains any special provisions in respect of computer generated evidence. Reference should be made to sections 8 and 9 of the CEA for further detail.

8.2 Electronic disclosure

When legal proceedings are issued against an organisation, or it is put on notice that proceedings are contemplated, the organisation has a duty to the court to preserve every document that is relevant to the claim. If records are destroyed in the knowledge that legal proceedings may be issued, a judge is likely to make adverse inferences against such destruction if proceedings are in fact commenced, as in the *McCabe* case referred to above.

Standard disclosure of documents under Part 31.6 of the CPR requires disclosure by a party of documents on which he relies, and documents which adversely affect his own case, adversely affect another party’s case, or support another party’s case.

Rule 31.7 of the CPR provides guidance on the scope of a search for documents and provides:

“(1) When giving standard disclosure, a party is required to make a reasonable search for documents

(2) The factors relevant in deciding the reasonableness of a search include the following –

(a) the number of documents involved;

the nature and complexity of the proceedings; the ease and expense of retrieval of any particular document; and

the significance of any document which is likely to be located during the search.

(3) Where a party has not searched for a category or class of document on the grounds that to do so would be unreasonable, he must state this in his disclosure statement and identify the category or class of document.”

As a recognition of changing times and the increase in electronic communication, the CPR were made the subject of recent amendments in October, 2005. The effect of the changes (set out in the Practice Direction under Part 31 of the CPR) is to place an obligation on a party not just to comply with the previous rules on search and disclosure above, but also requires that party to state whether in its search for documents it has searched :

- databases;
- backup tapes;
- mobile phones;
- notebooks;
- PDA devices;
- portable data storage media;
- servers;
- off site storage laptops; and
- handheld devices,

for electronic documents that may be relevant to the issues.

8.3 Ability to retrieve e-mails

As illustrated by rule 31.7(2)(c) of the CPR, the ability to retrieve e-mail within the timeframe specified by a particular rule or regulation is vital to compliance. Many organisations fail to realise the importance of retrieval and have been fined, not because they did not keep the requested e-mails, but because they could not be produced in the timeframe demanded. Some organisations have discovered this to their cost, whereas others have preferred to pay the fines rather than pay the sums required to an outside agency to locate the e-mails. In the United Kingdom, we have seen fines by regulators ranging from £1 million to £2 million: Abbey Life Assurance Company Limited was recently fined £1 million by the Financial Services Authority, part of which related to the inadequate maintenance of records. The detailed E-mail Management report published by the Butler Group in September 2004 cites further examples of the consequences of failing to have suitable systems in place:

- Norwich Union was forced to make an out-of-court settlement of £450,000 after it was alleged that its staff had sent defamatory e-mails about a competitor. By the time proceedings were issued, the e-mails had been deleted;
- one Fortune 500 company had to spend US\$750,000 to locate e-mails from an archive in response to a subpoena for discovery; and
- in the US, companies have been fined between US\$10 million and US\$100 million for not having adequate information retrieval procedures in place.

However, all the above examples have been recently overshadowed by the record judgment against Morgan Stanley in late 2005 (*Coleman (Parent) Holdings Inc v Morgan Stanley & Co Inc [2005]*). In a US\$30 million claim brought against Morgan Stanley, the court awarded damages against Morgan Stanley in the region of US\$1.58 billion (a significant proportion of which comprised punitive damages), the largest ever award issued for inappropriate data management. In this case Morgan Stanley was unable (and unwilling) to retrieve and disclose relevant e-mails requested by Coleman within the timeframe specified by the court.

It should be noted that fines issued in the United Kingdom are not generally of the magnitude as those imposed in the United States which has a culture of punitive fining and damages, although there are indications that the authorities are becoming more stringent in the United Kingdom. Firms should, therefore, be aware that regulatory bodies have the power to impose significant fines for any breach of a regulatory obligation. It follows that e-mails must be capable of being retrieved from whatever medium they are stored on. It is the responsibility of firms to be able to produce information when required, no matter how the information is stored.

The recent US case of *Zubulake v UBS Warburg* 217 F.R.D. 309 (S.D.N.Y. 2003). acts as a warning to law firms in this country as to the importance of ensuring systems are in place which can efficiently retrieve electronic communications. During a preliminary hearing of *Zubulake*, the Judge held that UBS Warburg was required to disclose all relevant e-mails in legal proceedings brought against it, despite the fact that these were stored on backup tapes from which it was difficult and, therefore, expensive to retrieve the relevant information. Further, UBS Warburg was ordered to produce the e-mails at its own cost. It is considered that judges in this country are likely to follow the reasoning in this case and will not allow firms to claim that the technology they use is inadequate as a reason to refuse a request for disclosure in legal proceedings.

It follows that a firm will not be able to hold the vendor of an electronic information management system responsible for the retrieval process, if it receives such a request, where the system has subsequently become out of date. It is the firm's responsibility to ensure it employs up-to-date software. Firms should be aware that the cost of retrieving e-mails from a system which does not include suitable software which fully controls the storage and retention of electronic documents can be greater than the cost of such a system (see the examples above).

To avoid such costly exercises, it is in the interests of firms and their IT directors to regularly evaluate the efficacy of their software systems and whether their existing systems meet the firm's requirements.

8.4 Code of practice for legal admissibility and evidential weight of information stored electronically – BIP 0008 (www.bsonline.bsi-global.com)

Compliance with the Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically (BIP 0008) will assist the firm in ensuring that electronic records are admissible in the United Kingdom and are also given due weight. Compliance with the Code does not, however, guarantee legal admissibility but defines best practice.

The Code particularly addresses the technical issues of:

- authenticity (trustworthiness of original and evidential content – it is important to be able to demonstrate that the computer system has been functioning properly in order to authenticate data stored on the system);
- integrity (retention of the evidential content of the information); and
- availability (accessibility of the information as required),

and can be used to demonstrate that output from an information management system is a true record of what was imported.

The Code provides practical examples and describes how it may be demonstrated to a court that the content of a specific data file created or existing within a computer system has not changed since the time of storage. It also sets out how it may be shown that where the data file contains a digitised image of a physical original document, the digitised image is a true facsimile of that original document.

The Code is structured in accordance with the five principles defined in “Principles of Good Practice for Information Management”, BSI-DISC PD 0010. These principles, which act as guidelines for the procedures and controls required, are:

- recognise and understand all types of information;
- understand the legal issues and execute duty of care responsibilities;
- identify and specify business processes and procedures;
- identify enabling technologies to support business processes and procedures, and
- monitor and audit business processes and procedures.

8.5 Code of practice for electronic documents and e-business transactions for evidence, audit and long-term duty of care – PD 5000 part 2

See : www.bsonline.bsi-global.com

BIP 0008 should be read in conjunction with PD DISC 5000. PD 5000 is a less practical Code and is primarily concerned with the authenticity, integrity and availability of electronically communicated information and the demonstrable levels of certainty required by an organisation. It is particularly applicable where the communicated information may be used as evidence both inside and outside the legal system.

The Code sets out the key requirements for electronic messaging, being:

- sender authentication: proving the identity of the sender;
- integrity: ensuring that the content of the electronic communication is what it purports to be;
- identity: identifying the electronic communication;
- identifying date and time of communication;
- confirming receipt;
- date and time of receipt: identifying the time of delivery and collection, and
- recipient authentication: proving the recipient's identity.

8.6 Information security management – British Standard 7799

See: www.bsonline.bsi-global.com

ISO 17799 and BS 7799, codes of practice for information security management, recognise that information is an asset which, like other important business assets, has value to the firm and consequently needs to be suitably protected. Information security is fundamentally about the preservation of confidentiality, integrity and availability of information. Security is key when discussing legal admissibility issues. Certain questions should be addressed, such as: when the electronic information was captured by the storage system, was the process secure; was the correct information captured and was it complete and accurate; during storage was the information changed in any way either accidentally or maliciously? Compliance with BS 7799 should help to ensure that electronic records may be given due weight.

Other than preserving the admissibility and evidential weight of electronic documents, securing documents and controlling access to information is vital for a number of other reasons including:

- legislation, such as the market abuse regulations, requiring law firms and their clients to provide details of all individuals who have had access to certain matter information;
- reducing the possibility of conflicts of interest arising within a law firm (see *Marks & Spencer plc v Freshfields Bruckhaus Deringer* [2004] EWCA Civ 741);
- maintaining the integrity of information barriers;
- compliance with the new Solicitors Practice Rules (Rules 16D and 16E) (introduced in May, 2006) regulating conflicts of interest and the duties of confidentiality and disclosure;
- client expectations in respect of confidentiality, and
- issues relating to the recent conversion of a number of law firms to LLP status.

Law firms and their clients, therefore, need to establish and implement a comprehensive Information Security Policy. BS 7799 sets out the requirements and helps to identify, manage and minimise the range of threats to which information is regularly subjected. The major point to the standard is that it covers both technology and business process and practice. A firm using BS 7799 as the basis for its Information Security Management System can become registered with the British Standards Institute. Registration demonstrates the firm's

commitment to information security and is likely to be demanded of law firms by clients in the future. To date, however, very few United Kingdom law firms have achieved accreditation.

8.7 Guidance

It is recommended that IT Directors review the standards of practice outlined above when updating their information management strategies and adhere to these standards where possible, although accreditation is not essential.

It should be noted, however, that compliance with these standards alone will not guarantee that a firm's information management policy will be foolproof, or that their electronically created and stored documents will be admissible as evidence.

9 Data Protection Act 1998

The Data Protection Act 1998 (**DPA**) regulates the way in which data relating to individuals may be processed. Processing data includes the storage of such data. The DPA is predominantly concerned with data in electronic form. The eight data protection principles can be briefly summarised, in that personal data should be:

- 1 processed fairly and lawfully;
- 2 processed for limited and defined purposes;
- 3 adequate, relevant and not excessive;
- 4 accurate and up to date;
- 5 kept for no longer than necessary for the purposes for which it is processed;
- 6 processed in accordance with the individual's rights;
- 7 secured against unauthorised processing and accidental loss or damage, and
- 8 transferred only to countries that have adequate levels of data protection.

It may be necessary to amend, delete or expunge specific information from information management systems as a result of court orders or to meet the requirements of the DPA. The information management system will also need to have the facility to amend incorrect data or remove irrelevant data held in contravention of the DPA.

In terms of the document management policies of law firms and the advice to be given to their clients, the following issues should be considered in order to comply with the DPA:

- If there is no good reason to keep personal information, it should be deleted (principle 5).
- Policies should identify particular categories of documents containing personal data as having specific retention periods with reference to any relevant statutory or regulatory requirements. For example, wording such as "documents relating to payments made to employees to be retained for 6 years pursuant to section 15 of the Taxes Management Act 1970" ensures that there is no conflict between principle 5 of the DPA that personal data is kept for no longer than is necessary and regulatory or other legitimate requirements to retain information.
- Policies should be put into practice to review documents to ensure that such documents are destroyed as soon as the retention periods stipulated expire.
- The law firm should make an assessment if it decides to keep certain client and matter related information beyond the necessary retention period. The firm will need to justify the continued storage of personal data.
- As individuals have the right to make subject access requests for personal data held about themselves, firms should ensure that their systems enable extraction of all the information relating to particular individuals without difficulty. The Information

Commissioner has stated that an organisation cannot blame the technical shortcomings of its systems as a defence for its failure to provide sufficient information.

- The Court of Appeal in *Durant v Financial Services Authority [2003] EWCA Civ 1746* refined the definition of “personal data” as “*information which affects [a person’s] privacy, whether in his personal or family life, business or professional capacity.*” When dealing with a subject access request, the firm can therefore limit the scope of the search by considering whether the information is capable of having an adverse impact on the individual, rather than being required to disclose every document that refers to the individual.

Despite the guidance given above, it should be pointed out that it will be difficult for firms to fully comply with all the DPA’s requirements. For example, unless every individual deletes every personal e-mail they send and receive from the system on a daily basis, personal data will be stored on backup tapes. As a result, most firms will struggle to comply with principle 5. Accordingly, each firm should appoint a partner who has overall responsibility for ensuring that the firm’s obligations under the DPA are met.

10 Copyright

It is a criminal offence under the Copyright, Designs and Patents Act 1988 (**CDP**) to make unlawful copies of material subject to another’s copyright. You may not copy or ask others to copy anything, whether for internal or external use, except as set out by the provisions of the CDP. The rules apply to e-mails and the internet as well as to hard copy documents. Storing work on, or scanning it to, an electronic document management system is an act of copying. As a guide:

- the general rule is that a document may not be scanned to an electronic document management system if the scanning of that document is not permitted under copyright law;
- whether or not the scanning is permitted depends on whether it falls under one of the exceptions to the general rule;
- the main exception which will permit law firms to scan documents is that they have *implied permission or consent* to scan the document. In these circumstances, implied permission derives from the idea that it is accepted business practice to store documents electronically and keep them for further reference; implied consent derives from the idea that during a matter the author of a document relating to the matter expects it to be copied for the purposes of the matter, and
- implied permission or consent will not apply to journals, magazines, newspaper cuttings or anything which has a copyright mark on it.

The copyright rules are extremely complex and, prior to introducing an information management strategy, advice should be sought from the copyright experts within the firm.

11 Guidance on statutory and regulatory retention periods

The types of documents that have to be retained and the periods of retention will partly depend on the nature of the particular business, legislation, regulatory bodies and best practice guidelines. These retention periods are, however, rarely clear-cut, as demonstrated below:

- Accounting records: Section 222(5) of the Companies Act 1985 states that records relating to company accounts must be retained for at least 6 years from the date they were created in the case of public companies, and for at least 3 years in the case of a private company. These periods are, however, subject to separate legislation such as the Taxes Management Act 1970, under which the Inland Revenue can conduct tax liability investigations. Under sections 34 and 36, for example, if there are reasonable grounds to believe that tax has not been paid due to negligent or fraudulent conduct, a person or

business is required to make available for inspection all relevant documents for a period of 21 years after the end of the accounting period to which the investigation relates.

- Employee records: Section 15 of the Taxes Management Act 1970 requires an employer to retain all documents relating to payments made to employees for 6 years. In addition, regulation 55 of the Income Tax (Employments) Regulations 1993 (SI 1993/744) requires employers to retain records relating to the calculation of pay for at least 3 years after the end of the year to which they relate.
- Limitation periods: Legislation exists to provide cut-off points, beyond which a legal action cannot be issued. This is to ensure that an organisation or individual does not have indefinite legal liability. The degree of risk the organisation is willing to take when deciding how long to retain documents should be considered in developing a retention and disposal policy. A balance should be struck between the cost of retaining documents, whether stored electronically or physically, and the comfort of keeping documents. The organisation needs to assess the risk that it may need to defend itself against the threat of litigation, or it may need to retain documents to initiate legal action at some point in the future. Conversely, choosing to retain documents beyond their statutory retention period carries its own risks. Such retention may be in breach of the principle 5 of the DPA if documents contain personal data and the purpose for which that information was obtained no longer applies. In addition, documents which are kept beyond their retention periods will remain disclosable in litigation.

As, in many cases under the Limitation Act 1980, there is a limit on the period in which legal proceedings can be issued, businesses can, in theory, make informed judgments on how long to retain certain types of document. As a guide, the time limits for making a claim are as follows:

- actions for breach of contract – 6 years from the date of breach for simple contracts (section 5) and 12 years if the contract is under seal (section 8);
- actions in relation to sums which can be recovered under statutory provisions – 6 years from the date the debt was incurred (section 9);
- personal injuries arising from negligence – 3 years from the cause of action, or 3 years from the date on which the injured person became aware that the injury caused by the other party was significant (section 11), and
- product liability – 10 years from the date of supply (section 11A).

For further detail see *Andrew C Hamer "The ICSA Guide to Document Retention"*, (ICSA Publishing Ltd., 2004) and *Stephen Mason "E-mail, networks and the internet: A concise guide to compliance with the law"* (xpl publications, 6th edn, 2006) ISBN 1 85811 3563".

It should be borne in mind, however, that some limitation periods can be more open-ended. In personal injury cases arising from negligence, it can be many years before a claimant becomes aware that he or she has sustained an injury or that it is significant for the purposes of section 11 (for example, in cases where exposure to asbestos causes lung cancer or CJD is contracted from contaminated meat). In addition, section 33 of the Limitation Act 1980 gives judges discretion to waive the time limit in which to bring a personal injury claim in certain circumstances altogether. This uncertainty makes it difficult for businesses to make a practical judgment as to the period for which documents are retained.

- Professional indemnity cover: Where it is believed that a relevant limitation period has expired, law firms should remember to consult their professional indemnity insurer to check the duration of record keeping obligations under the insurance contract before documents are destroyed. This will ensure that cover remains in place in the remote event of a claim being brought in these circumstances.
- Financial Services Authority regulations: The Financial Services Authority's Conduct of Business Rules contains document retention provisions that apply to firms conducting investment business. Certain clients of law firms will often fall into this category. In many cases the requirement is to retain client records for six years, but reference should be made to the detailed provisions to determine requirements for particular classes of

document. In some cases documents are required to be kept indefinitely. For further information please see <http://www.fsahandbook.info/FSA/Handbook.jsp>.

- Law Society rules of professional conduct: The Law Society of England and Wales does not prescribe a time period for the retention of client matter files. The Law Society booklet "Guidance – ownership, storage and destruction of documents", dated December 1986 and revised February 1999, advises that all files should be kept for a minimum period of six years after completion of the matter. Please refer to http://www.lawsociety.org.uk/documents/downloads/Profethics_Docs.pdf for more detail.

12 Best Practice Guidelines

There are a number of sources of best practice guidelines available regarding the management of electronic information and records. Additionally, the increased awareness of electronic document management and retention tools in the legal sector is resulting in the development of specific legal industry best practice.

12.1 International Standards Organisation (www.iso.org)

The International Organization for Standardization (ISO) has produced a standard ISO 15489 covering information and documentation records management. It consists of two papers

- [ISO 15489-1:2001](#) : Information and documentation -- Records management -- Part 1: General
- [ISO/TR 15489-2:2001](#) : Information and documentation -- Records management -- Part 2: Guidelines

ISO 15489 sets out the methodology for introducing an end-to-end document and records management process. It is more than technical, covering policy, practice and procedure and so serves as a useful source of information for records management on an international scale.

See

<http://www.iso.org/iso/en/CombinedQueryResult.CombinedQueryResult?queryString=15489>

12.2 *The Model Requirements for the Management of Electronic Records Specification*

The Model Requirements for the Management of Electronic Records (MoReq) specification was prepared for the iDA (Interchange of Data between Administrations) programme of the European Commission. It focuses mainly on the functional requirements for the management of electronic records by an Electronic Records Management System (ERMS).

This specification is equally applicable to public and private sector organisations which wish to introduce an ERMS, or which wish to assess the ERMS capability they currently have in place.

While the specification focuses on functional requirements, it recognises that non-functional attributes are central to the success of an ERMS, as with any information system. However, these non-functional attributes vary enormously between environments. Accordingly, they are identified but described only in outline.

- See <http://ec.europa.eu/idabc/servlets/Doc?id=16842> explaining the practical application of MoReq
- See <http://ec.europa.eu/idabc/servlets/Doc?id=16847> for the full specification

12.3 The National Archives Functional Requirements for Electronic Records Management Systems (ERMS)

The National Archives has published two sets of functional requirements to promote the development of the electronic records management software market, and has run a programme to evaluate products against the 2002 requirements. Whilst these requirements were initially formulated in collaboration with central government, they have been taken up with enthusiasm by many parts of the wider public sector in the UK and in other parts of the world.

The national archives website is a useful source of information.

See <http://www.nationalarchives.gov.uk/electronicrecords/function.htm>

12.4 Butler Group report on e-mail management (www.butlergroup.com)

This report was published in September, 2004 with a view to providing guidance on reducing corporate risk and unlocking value through e-mail lifecycle management. The report suggests a number of best practices regarding the management of e-mails (which can also be applied to the management of other electronic documents) including:

- e-mail management should be taken out of the hands of the employees;
- organisations need to determine how long to retain e-mails by measuring the value contained within them against the risk of litigation by retaining them beyond their retention period;
- if employees are using their mailboxes as a knowledge management solution, then in order to derive full value from knowledge contained within e-mails, users must be allowed to search archives for information contained within their own e-mails. At the same time sensitive e-mails must be protected from unauthorised access. Policies need to be implemented to control access to e-mails in the archive;
- spam should be eliminated before it reaches the mail server to ensure that workers are not burdened by spam. Quarantining blocked e-mails and either allowing employees to check their own or appointing an administrator to decide which are genuine e-mails will eliminate problem of false positives;
- the personal use of e-mail should be limited;
- strategies should be put in place for retrieval of historic e-mails with appropriate search technologies, even if this is not required for compliance purposes;
- it should be ensured that e-mails can be retrieved from whatever medium they are stored on;
- larger organisations that are subject to regulations should appoint a compliance officer who must liaise with e-mail administrators to ensure that all aspects of e-mail management comply with requirements of the regulators. The compliance officer must also liaise with business managers who will also be subject to legislation that may affect e-mail;
- administrators need to ensure that any downtime is within acceptable limits so that end-users are not unduly affected. Organisations need to consider putting systems in place to allow minimum downtime e.g. clustering; and
- corporate e-mail systems must be included in disaster recovery and business continuity planning with the level of availability that reflects its criticality to the business.

12.5 ARMA

ARMA International is an internet based association, which can be found at <http://www.arma.org>, and is a gateway to information on managing both paper and electronic records. ARMA offers resources such as:

- legislative and regulatory updates;
- standards and best practices;
- technology trends and applications;
- live and web-based education;
- marketplace news and analysis;
- books and videos on managing records and information; and
- global network of 10,000+ records and information management professionals.

The site provides links to products such as online self-assessment tools which allow an organisation to determine whether its electronic document management system is as effective as it should be by comparing it to best practices. Articles can be downloaded on issues such as electronic disclosure, systems design requirements, regulatory compliance, case studies and reviews of software packages.

12.6 *The Sedona Guidelines: Best practice guidelines & commentary for managing information & records in the electronic age*

See: <http://www.arma.org/pdf/articles/SedonaRetGuide200409.pdf>

Specifically, on the ARMA site, the Sedona Conference Working Group agrees that the subject of information management and record retention is of critical importance in the digital age. The guidelines suggest a number of best practices regarding the management of electronic information including specifying that an organisation:

- should have reasonable policies and procedures for managing its information and records;
- should put in place information and records management policies and procedures which are realistic, practical and tailored to the circumstances of the organisation;
- need not retain all electronic information ever generated or received;
- adopting an information and records management policy should consider including procedures that address the creation, identification, retention, retrieval and ultimate disposition or destruction of information and records; and
- policies and procedures must mandate the suspension of ordinary destruction practices and procedures as necessary to comply with preservation obligations related to actual or reasonably anticipated litigation, regulatory investigation or audit.

12.7 *The Commercial Litigators' Forum: Electronic Disclosure (27 October 2004)*

See: <http://www.commerciallitigatorsforum.com>

This paper suggests the following best practice guidelines when dealing with disclosure of electronic documents during litigation. Each party should:

- identify the nature and scope of the search for electronic data which is reasonably likely to contain relevant information in order to comply with CPR part 31 and the overriding objective;
- identify the nature of the information required from their respective clients;

- ensure that clients have been advised and have taken measures to preserve potentially disclosable data from inadvertent alteration or destruction;
- identify the scope of the search for information in terms of individuals who may hold data and the appropriate time frame when potentially relevant data may have been created;
- identify the range of electronic data (e.g. readily accessible data, back-up data and residual data etc.) to be searched for the information sought;
- identify the key words or concepts to search and consider whether limitations should be imposed on searches;
- identify the types of files to be searched (e.g. e-mails, Word files, PowerPoint files etc.);
- identify the hardware on which data may exist (PCs, servers etc.);
- consider whether searches of back-up data should be made, and if so, which party should bear the cost;
- consider the need to instruct IT experts to carry out searches if data not readily accessible; and
- set a timetable for conducting such searches.

13 Emerging industry best practice regarding electronic document management and retention

13.1 Industry best practices

A number of law firms are implementing electronic document management systems with a view to increasing efficiency, improving the management of the firm's information, easing searching, accessing and retrieval of information, and assisting in addressing its risk management and compliance issues. The following are now being adopted by a number of firms to manage their client-matter files and so may arguably be considered best practice:

- all matter related information should be filed on the appropriate electronic matter file to the extent that it is practicable and not prohibited by law or other reason (e.g. copyright restrictions);
- any matter related information not stored on the appropriate electronic matter file should be stored on a related and referenced paper file using a suitable firm-wide client matter code;
- all matter related information stored on a paper file should be referenced to and indexed on the appropriate electronic matter file;
- firms should consider which original documents should be retained on the paper file for regulatory or evidentiary purposes. Given the Law Society's revised 2005 E-mail Guidelines for Solicitors, it is not necessary to include clean copies of electronically created and stored documents on the paper file;
- e-mails should not be printed and stored on the paper file but instead should be filed on the electronic matter file;
- consideration should be given to creating a forensic / audit trail for e-mail as deletion and expunging of information between backup cycles means that no record is kept. Some e-mail systems have journaling functions or external systems are available to do this. The choice of system will be down to the degree of "tamper proofing", budget and functionality required;
- the use of any new communications technology (such as Blackberries, PDAs or instant messaging) should be treated in exactly the same way as e-mail or other formal

documents and firms should look to revise policy and systems management to cover new technology before it is launched for business use;

- the matter file will constitute both the electronic matter file and the paper matter file as well as any other items stored in respect of the matter and referenced on the electronic file;
- the Law Society's revised E-mail Guidelines for Solicitors advises that "where some correspondence about a matter is stored electronically and the rest is on paper, firms should ensure that none of the material will be overlooked if responsibility for a matter is transferred (perhaps temporarily). Firms should also be confident that they know what information their systems record. If not, an audit may be appropriate";
- matter related information, both in electronic and paper form, should only be accessible by those people who are required to obtain access to it. A number of firms are therefore implementing matter security which means that only the matter team has access to the electronic matter file and information stored within it;
- the electronic document management system should include a version control system enabling a record of changes made to a document to be kept with the ability to review and retrieve previous versions of the document after it is created, and
- explanatory comments must be included when creating a new version of an electronic document detailing the reasons the changes are being made.

Technology only provides part of the solution. Without effective business processes and procedures in place such as those highlighted above, and without the successful implementation of these practices, the benefits of any information management strategy will never be fully realised.

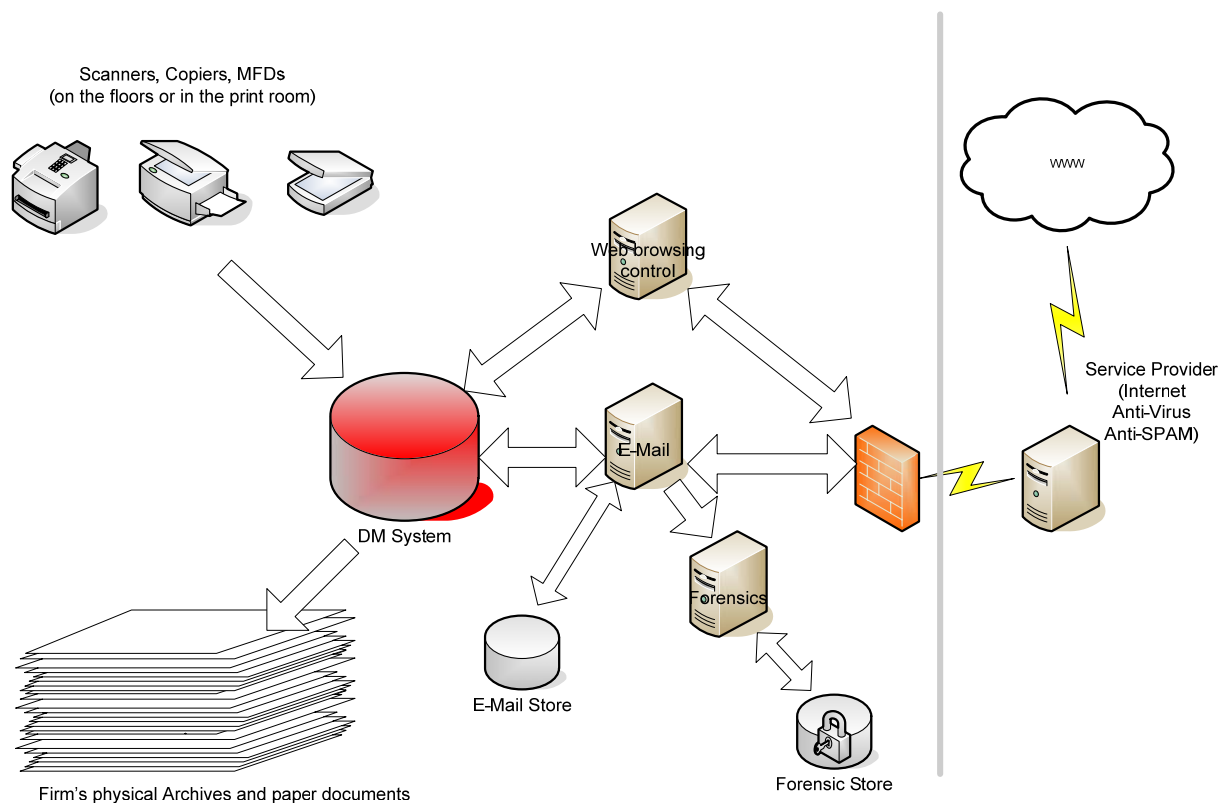
13.2 Proposed model

The diagram below illustrates a model that is emerging as best practice within the legal sector. Each element of the model is then briefly discussed. This is only one model. There are many models and each element may have to be varied in line with the size, structure, technology or budget of the particular organisation.

When designing an information management system it is important to consider that the more time that elapses between creating, sending, receiving or working on a document and when a document is filed, the less likely it is to be filed or filed in the right place. As such, the system design should allow (and possibly encourage) system users to archive files in a suitably managed electronic storage system as soon as is practically possible.

To achieve this, the key "code" that is used for filing (generally client and matter code) should be available immediately after the conflict and anti-money laundering checks have been completed and systems should be avoided that have delays between the completion of these checks and the creation and propagation of the client-matter code throughout all systems for immediate use. These codes then allow an accurate record of any time recorded or documents created whether or not your firm proceeds with the matter.

Emerging Best Practice Model



The Model Explained

- The central “hub” of the system is a single document management system (**DMS**) from a reputable vendor (by single we mean one system, it may be distributed provided an “always up to date” master record exists which is considered the client-matter file). In this DMS all documents relating to a client-matter and that can be stored in an electronic DMS will be stored, including all client-matter related e-mails. Anything that cannot be scanned (e.g. deeds etc.) is held in a physical store managed by a linked system from a reputable vendor with cross references between the two systems. Additionally, to be fully utilised by a law firm, the system should be flexible enough to be used for all support services (e.g. IT, Marketing, Finance and Facilities) and should work equally as well for them allowing them use of coding structures for general and project based document filing.
- The e-mail system is closely linked to the DMS to make it easy for users to move documents between the two systems and to store e-mails and attachments under the firm’s client-matter referencing system in the DMS. Mail box quotas encourage staff to file important client-matter related e-mails into the DMS but the firm’s policy adequately defines what must be carried out in respect of filing client-matter related information. Spot check audits of client-matter files are regularly performed to ensure documents are being filed in the central DMS repository in a timely manner.
- The DMS is “partitioned” to allow different retention and destruction policies to be applied (e.g. finance and HR records are stored in different areas or metadata is used to differentiate record types). This permits archiving to maintain differential retention periods for compliance purposes.
- DMS and archive system security policies are in place and access control mechanisms are strictly controlled to ensure all security (including commercial Chinese walls) are in place. It may be appropriate to employ external security specialists to attempt to penetrate systems from the outside and inside your organisation.

- A forensic system (or e-mail journaling) captures all e-mails and instant messaging in or out of the firm and within the firm. This enables fast responses to data subject access requests under the DPA, litigation, client issues or any other issue requiring evidence of delivery or non delivery. The firm's information management policy makes it clear that the forensic or journaling system is not to be used as a client-matter archive.
- Any physical paper is scanned to the DMS in electronic format. It may be kept for whatever period is necessary for compliance or resilience until integrity is checked and backups taken. It should be noted that scanned documents go to the DMS, not to e-mail, and documents to be sent outside the firm must be scanned to the client-matter file in the DMS prior to being sent, for record keeping purposes.
- Anti virus is installed on the e-mail system, all servers and PCs but additional anti-virus and anti-spam solutions may be outsourced. Systems are in place for staff to check incoming blocked mail and have it sent to their Inbox if they discover blocked business mail. Administrators regularly monitor false positives and adjust anti spam filtering levels accordingly.
- Web browsing is monitored. Unsuitable sites are blocked and downloads restricted. Necessary downloads, however, are virus scanned and encouraged or forced to be stored in the DMS. This discourages social or trivial use and ensures proper records management.
- Policy considerations:
 - The firm's system is defined and explained to all employees, and processes are in place to train all staff and identify and train all new joiners.
 - The employment handbook, together with the e-mail policy, explains to what extent web browsing and e-mail can and cannot be used and explains the purpose, function and facilities of any forensic or monitoring systems in place, clearly highlighting that web sites viewed and e-mail sent or received may be viewed by management and supervisors given due cause.
 - Retention and destruction policies are clearly defined and staff educated as to what the policies are, what to do and how to do it. Incentives are in place to recognise excellence in this area.
 - The rationale and approval process behind the policies are recorded in case the policies are questioned in the future and audits of compliance with the policy in the firm together with records of the audits and results should be kept. This will strengthen the commitment within the firm whilst at the same time acting as strong defence should your firm be questioned on its policy and management.
 - Data protection and copyright policies are clearly defined and staff educated as to what the policies are.
 - Terms of engagement limit the commitment of a firm to dispose of documents at a client's request.
 - Policies for handling ownership and management of files when staff leave the firm should be in place and ideally partners and other staff should be contractually responsible for the effective handover of all files prior to leaving the firm.

The model can be expanded depending on need and budget. Some examples are given below.

- **Client matter inception and auto generation of client-matter codes** – In a DMS it is normal to have a pending client-matter code for “no or new client-matter”. This is often due to the time taken to complete the required conflict and anti-money laundering checks and assign a client-matter code (generally issued from a practice management system “PMS”). Depending on whether the new client matter involves an existing or new client and the technology being used, the time from code request to code creation can be days during which time is generated and documents are created and filed under the “no or new client-matter” general code. Reducing the time from request to creation and dissemination

into the DMS, time recording and e-mail systems will reduce the amount of documents stored under the general code. This can be assisted by work flow solutions. Once the timeframe is reduced to hours or less, mechanisms to “mop up” files under the general code can then be implemented in effect forcing files to be allocated the correct codes. Often the issues raised above only face “best of breed solutions” as smaller, fully integrated PMS systems exist for the smaller firm. These integrated PMS systems provide client-matter codes immediately even before conflict and money laundering checks are carried out. The matter is of course flagged as such and account ledger creation is barred. Often limits of WIP are imposed to incentivise fee earners to complete regulatory procedures or provide commercial protection to the firm on matters that may not proceed but the DMS should never be locked down as the firm will always need to send out documents (for example to request money laundering documents)

- **Remote Access** – Filing e-mails in a DMS system can make them inaccessible to the travelling user. It is important to consider the ability to remotely access the DMS when designing the system, otherwise resistance to filing in the DMS will be inevitable.

It may be felt that the above technology model is the domain of the larger law firm but regulation for correct file management applies to all firms and the problem is the same even if the scale is not. Technology available for smaller firms often offer single systems, closely integrating the core elements and permitting solutions like the above to be achieved by small firms without investment in best of breed technology where pricing may be prohibitive. Such systems are available for even the smallest of practice.

13.2.1 Old data

One issue that all firms will face when implementing models like that outline above is “what to do with old data”.

Introducing a model that ensures appropriate levels of file management will, if implemented correctly, undoubtedly produce results from the date of introduction. However, a significant number of old matter files will remain outside the new model. In addition a number of these are likely to be active matters that have run for a period of time. It is essential that a firm undergoing change considers this issue as it should govern what policy is adopted and even the implementation methodology.

There is no right or wrong way however various elements must be considered:

- **Known date** – firms should ensure that it is simple for staff to know where to look for archives. Often this is date dependant in that those records that are “pre-system” will be in “the old method” and those post-system will be in the new. Implementing the migration of different records at different times can considerably complicate matters and in an ideal World users should be able to say “records before x [date] are in x system and after that date they are in y system”
- **Consider a “look up”** – Although a general date rule as above may apply governing whether a matter is managed in an old system or a new, often there are complications such as spanning matters (see below) and other issues and a reference point for all matters to be able to ascertain under what system it is managed is advisable. As the new system will become the defacto standard in time for all matters, it may be advisable simply to load all existing client and matter codes into the new system (but not the records themselves – just the “index” or meta data) with indication in the profile or metadata as to under what system the matter is managed possibly with instruction or pointers as to how to search for that matter if not managed in the new system. This will mean that a user can search in the new system for any and all records however the new system may on occasion refer them to alternative, older storage systems. This prevents confusion as to where to start looking for a firm’s records.

- **“Spanning” matters** – a policy decision must be taken and enforced as to what to do with matters that span implementation dates. It is generally not advisable to have part of a matter on the old system and part on the new and it is advisable to either import all documents on a spanning matter into the new system or run with it on the old until complete. The decision will often depend on the practicalities of being able to import into the new system existing documents and also how long the matter is likely to run past the implementation date of the new system.

Even in an ideal solution where it is technically and economically possible to import all records from older systems, it is likely that considerable paper files will exist and so it is unlikely that the perfect solution of one system is achievable. That said it is important to ensure that the management method of a matter is clear and evident, that matters are not, as far as is possible, managed under two systems and that all new matters adhere strongly to new systems, policy and procedures.

14 Acknowledgements

Authors -

- Peter Owen – Director, LITIG / Director, Lights-On Consulting Limited
- Sam Suri - Director, It Matters Consulting Limited

Key Contributors

- Stephen Mason - member of the IT Panel of the General Council of the Bar of England and Wales

Other Contributors

- Tim Hill - Law Society of England & Wales
- The authors would like to thank all Litig members (particularly Jan Durant of Lewis Silkin and David Coates of Bond Pearce), legal IT Directors, suppliers and others that have provided input, feedback and comment on the document the numbers of which are too numerous to list.

15 Document Control

RELEASE 1 (Versions 1-11) - Version 11 released for public comment October 2005

RELEASE 2 (Versions 12 – 19) – Version 19 released to the public on 10th October 2006

The views, recommendations, policies and other comments in this document are those of the individual members to which they are attributed and are not to be construed as being those of the firms or organisations which those members represent. For the avoidance of doubt, all such views, recommendations, policies and comments are made or given on an informal and nonbinding basis, for the purposes of LITIG Limited and not for any other reason, and accordingly neither LITIG Limited nor the member in question shall have any responsibility or liability for any loss or damage arising from the use of or reliance on such views, recommendations, models or opinion.