# Trademarks

Document Manager and Document Manager Administration are trademarks of Document Logistix Ltd. TokOpen, TokAdmin, TokImport and TokExRef are registered trademarks of Document Logistix Ltd. All other trademarks acknowledged.

# Copyright Statement

Copyright © 1999 to 2013 by Document Logistix Ltd. All rights reserved. Guide to Document Management, 2013.

No part of this document may be reproduced, copied or transmitted in any form or by any means without the written permission of Document Logistix Ltd.

Document Logistix Ltd believes that the information in this document is accurate at the date of release but accepts no responsibility for any loss arising from omissions or inaccuracies contained herein. Information within this document is subject to change without notice.

For more information on this or other Document Logistix products, please contact Document Logistix Ltd.

# Contact Details

<table>
<thead>
<tr>
<th>Document Logistix Ltd – UK</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Main Address:</strong></td>
<td>8 Copperhouse Court</td>
</tr>
<tr>
<td></td>
<td>Caldecotte</td>
</tr>
<tr>
<td></td>
<td>Milton Keynes</td>
</tr>
<tr>
<td></td>
<td>MK7 8NL</td>
</tr>
<tr>
<td></td>
<td>United Kingdom</td>
</tr>
<tr>
<td><strong>Telephone Main Lines:</strong></td>
<td>(United Kingdom) (+44) (0)1908 366388</td>
</tr>
<tr>
<td><strong>Telephone Support Lines:</strong></td>
<td>(United Kingdom) (+44) (0)1908 366722</td>
</tr>
<tr>
<td><strong>Email Information:</strong></td>
<td><a href="mailto:info@document-logistix.com">info@document-logistix.com</a></td>
</tr>
<tr>
<td><strong>Email Support:</strong></td>
<td><a href="mailto:support@document-logistix.com">support@document-logistix.com</a></td>
</tr>
<tr>
<td><strong>Fax:</strong></td>
<td>(United Kingdom) (+44) (0)1908 367700</td>
</tr>
<tr>
<td><strong>Web:</strong></td>
<td><a href="http://www.document-logistix.com">www.document-logistix.com</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Document Logistix LLC – USA</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Main Address:</strong></td>
<td>3616 Far West Boulevard</td>
</tr>
<tr>
<td></td>
<td>Suite 117-309</td>
</tr>
<tr>
<td></td>
<td>Austin</td>
</tr>
<tr>
<td></td>
<td>TX 78731</td>
</tr>
<tr>
<td></td>
<td>USA</td>
</tr>
<tr>
<td><strong>Telephone Main Lines:</strong></td>
<td>(USA) 1-512-345-4600</td>
</tr>
<tr>
<td><strong>Email Information:</strong></td>
<td><a href="mailto:us.sales@document-logistix.com">us.sales@document-logistix.com</a></td>
</tr>
<tr>
<td><strong>Email Support:</strong></td>
<td><a href="mailto:support@document-logistix.com">support@document-logistix.com</a></td>
</tr>
<tr>
<td><strong>Fax:</strong></td>
<td>(United States) (+1) (512) 233-2351</td>
</tr>
</tbody>
</table>
Software

This guide describes Document Management considerations in relation to the Document Manager software from Document Logistix Ltd.

This guide may not exactly reflect the software as it evolves, but core functionality remains the same.
# Contents

1 **PREFACE**................................................................................................................................. 1
   1.1 About this Guide ......................................................................................................................... 1
   1.2 Intended Audience ...................................................................................................................... 1
   1.3 Related Documents .................................................................................................................... 1
   1.4 Conventions ............................................................................................................................. 1
   1.4.1 Definitions .......................................................................................................................... 1

2 **DOCUMENT MANAGEMENT OVERVIEW** ............................................................................. 3

3 **OPERATIONAL CONSIDERATIONS** ......................................................................................... 4
   3.1 Freedom of Information Act (UK) ............................................................................................... 4
      3.1.1 Highlights ......................................................................................................................... 4
      3.1.2 Two Way Street ............................................................................................................... 5
      3.1.3 FACT Versus FICTION ................................................................................................... 5
      3.1.4 In Practice ....................................................................................................................... 5
   3.2 Data Protection Act ..................................................................................................................... 6
      3.2.1 The Eight Data Protection Principles ............................................................................... 7
      3.2.2 World Wide Web ............................................................................................................ 7
      3.2.3 Exemptions ..................................................................................................................... 7
      3.2.4 Rights and Recourse ....................................................................................................... 8
   3.3 Legal Admissibility ..................................................................................................................... 8
      3.3.1 Principal Guidance .......................................................................................................... 8
      3.3.2 Classification .................................................................................................................. 9
      3.3.3 A True Copy? .................................................................................................................. 9
      3.3.4 Keeping Current ............................................................................................................. 9
   3.4 Financial Regulation .................................................................................................................. 10
      3.4.1 Sarbanes-Oxley Act ........................................................................................................ 10
      3.4.2 Financial Services Act .................................................................................................. 11
   3.5 Technology .............................................................................................................................. 11
      3.5.1 Scanners ....................................................................................................................... 12
      3.5.2 Storage ......................................................................................................................... 12
      3.5.3 Standards ....................................................................................................................... 13
      3.5.4 Software ....................................................................................................................... 13
4 COMPANY POLICY .................................................................................................................................................. 15
4.1 What is a Document Management Policy? .................................................................................................... 15
4.1.1 Setting Up a Document Management Policy ................................................................................................. 15
4.2 Sample Document Policy .................................................................................................................................... 16
4.2.1 Introduction .......................................................................................................................................................... 16
4.2.2 Software Environment ......................................................................................................................................... 17
4.2.3 Document Creation and Naming Conventions .................................................................................................. 18
4.2.4 Document Versions .............................................................................................................................................. 18
4.2.5 Document Types, Profiles and Templates ......................................................................................................... 18
4.2.6 Storage and Distribution Formats ...................................................................................................................... 19
4.2.7 Document Types Restricted to a Drawer ........................................................................................................... 20
4.2.8 Drawer Structures ............................................................................................................................................... 21
4.2.9 Drawer-Specific Document Types .................................................................................................................... 22
4.2.10 Document Types with Regard to Emails .......................................................................................................... 22
4.2.11 Disposal of Documents and Document Retention Periods ........................................................................ 25
4.2.12 Physical Storage Locations and Secure Shared Drives .................................................................................. 26
4.2.13 Groups and Users .............................................................................................................................................. 26
4.2.14 Sample Permissions for Users and Groups .................................................................................................... 27
4.2.15 Sample Document Retention Periods ............................................................................................................. 30
INDEX ................................................................................................................................................................... 32
1 Preface

This section provides an introduction to this guide.

1.1 About this Guide

This guide describes the Document Management considerations an organisation should take into account when implementing the Document Manager document management system.

1.2 Intended Audience

This guide is intended for administrators and company planners responsible for designing, implementing and maintaining the Document Manager document management system.

1.3 Related Documents

For more information on the Document Manager document management system, refer to the following:

- Document Manager Installation Guide
- Document Manager User Guide
- Document Manager Administration Guide

1.4 Conventions

Throughout this manual, the following convention is used:

- Cross-references use italics; e.g. see 1.4 Conventions on page 1 for more information.

Additional information is provided using icons to draw attention to them:

NOTE: Notes are used to give useful supplemental information about the subject matter.

WARNING: Warnings are used to provide important pieces of information.

1.4.1 Definitions

The following terms are relevant to this guide:

- **Document Manager**: The Document Manager program from Document Logistix.
- **Document Manager Administration Module**: The Document Manager Administration Module enables system administrators to configure the Document Manager system.
• **Document Management Policy**: A set of guidelines to be drawn up before implementing a Document Management system and to be adhered to in company practices.

• **Drawer**: In Document Manager, drawers contain folders and documents in a similar way to filing cabinets that hold physical folders and hard-copy documents. Typically, drawers align to an organisational process or department (such as Human Resources).

• **Folder**: Folders group documents based on common criteria, which are defined in Document Manager using indexes.

• **Index**: An index is a field used to classify and identify a folder or document. There are default system index fields, such as ‘Doc Description’, and custom fields can also be created, for example ‘Supplier’. Users complete indexes to categorise documents and enable efficient searching.

• **Document Type**: Each document in Document Manager must have an associated document type, which is essentially a document category. Documents types can be defined based on document use as well as format.

• **Application Document**: Refers to a document in Document Manager that is associated with a PC application, for example a Microsoft® Office Word document. These documents will open in their associated application on a user’s computer.

• **Storage Location**: A location where document files are stored. In Document Manager, different storage locations can be defined, for example, for drawers or document types, and with different levels of security.

• **Version Control**: Allows a document to be saved as a major version or a minor version, enabling a record to be kept of changes to documents.

• **Audit Log**: A record of all actions taken in Document Manager, for example, actions taken on a specific document.

• **Permission**: Users are granted permissions to enable them to perform actions in Document Manager. This is a security measure and ensures only authorised people can carry out important or sensitive actions.

• **Check Out/Check In**: This feature ensures that only one version of a document is maintained. A user ‘checks out’ a document to prevent anyone else making changes to it, for example, to work on it away from the office.

Additional Document Logistix products are available to further enhance the document management process. For more information about them, please refer to our Website, [www.document-logistix.com](http://www.document-logistix.com) or speak to an authorised reseller.
2 Document Management Overview

The appropriate management of company documents is vitally important to an organisation. Efficient management of documentation can make it quicker and easier for employees to collaborate on tasks and save businesses significant amounts of money. Business documents also have legal weight and care must be taken to preserve their integrity during storage. The logistics of storage also plays an important role in business operations, both in terms of cost and the space required to host vast numbers of documents (both physical and virtual). The length of time documents are to be retained is also a critical factor.

This guide explains some of the considerations an organisation must take into account when implementing the Document Manager document management system from Document Logistix, including relevant legislation. This document also describes the importance of company management policies and includes an example policy that can be used as a starting point for your organisation’s own policy.
3 Operational Considerations

There is much legislation that affects the use of Document Management including some that is industry specific. As an organisation using Document Management, you should familiarise yourself with this legislation and ensure you are compliant with it. Furthermore, the ownership and use of Document Management software does not automatically ensure compliance.

This section details some of the important aspects of this legislation.

3.1 Freedom of Information Act (UK)

The Freedom of Information Act gives everyone the right to access information held by the public sector. This includes the government, local authorities and other publicly funded or owned organisations.

The Act was passed in 2000 and came into force in 2005. The Scottish Parliament enacted a similar set of legislation for Scotland. This Act also required changes to the Data Protection Act so that both sets of legislation were consistent. The Data Protection Commissioner had his powers widened to cover Freedom of Information and Environmental Information regulations, and is now known as the Information Commissioner.

3.1.1 Highlights

- There is a general right of access to information held in the public sector. Interestingly, it is not restricted to UK citizens, and no reason need be given when requesting information.

- Requests for information have to be in writing including email. The public authority is expected to respond within 20 working days in normal circumstances.

- Some 23 exemptions exist, covering items from national security to commercial confidentiality, most of which apply to central government.

- Public bodies have a duty to produce a publication scheme so that it is clear what is available, in what formats and whether or not there are any charges for access.

- Powers of enforcement and appeal are available through the Information Commissioner and an Information Tribunal.

- Certain historical documents are protected for periods ranging from 30 to 100 years.
3.1.2 Two Way Street

The legislation makes it explicit that the public authority has to provide every assistance to satisfy a request and that they should do so in a timely fashion. The authority can levy a reasonable charge for supplying the information and can also request clarification if the request is not sufficiently specific.

If a request is covered by an exemption, then this should be stated. If the request is unreasonable or vexatious, then the public authority is entitled to refuse the request. If an individual believes that the authority is not complying with its obligations, then there is a right of appeal.

3.1.3 FACT Versus FICTION

This legislation caused a considerable amount of confusion and misunderstanding even though the Act is clearly laid out. Principal amongst the misguided views were:

"There is no way that Freedom of Information and Data Protection can be reconciled."

FACT: The Act is clear. An individual has a right to all public information, save exempted material or personal data. If personal data exists in a document, it must be removed before the document is issued.

It is as simple as that.

"I only need disclose information created since the Act came into force."

FACT: All information, whenever created, is subject to the Act. Access to that information was granted in 2005. The word ‘information’ is used deliberately as many think of the Act relating solely to written documents. It is not. It applies to any information, however held, including audio, video, computer data, handwritten notes and more.

"I can destroy information I do not want published."

FACT: This was largely true in the past unless it was subject to litigation. It is now a criminal offense to destroy records to avoid disclosure. At the same time, an individual or organisation has a duty under the Data Protection Act to destroy personal information after it has served its useful purpose.

3.1.4 In Practice

The Act has been in force for some time now and a pattern is emerging as to its use. Yes, it is being used for the purpose intended. However, this appears to be the minority use. The majority of requests are commercially instigated, used for party politics or the Press in search of stories.

Clarification of grey areas is slow in coming as the Information Commissioner has a backlog of adjudications to make and to date has not made any landmark judgements or exemplary enforcements.
Public bodies have not been inundated with requests as at first feared. This is fortuitous as many were ill-prepared and simply held their breath to see what would transpire. Where it has had the greatest impact is that much more information is pro-actively made available, principally through Web sites. With this substantial body of information now available, it may become like finding a needle in a haystack to uncover some of the real gems.

### 3.2 Data Protection Act

Confusion over apparent conflict between the Data Protection and Freedom of Information Acts exists largely because each was drafted with different aims and in contrasting styles.

The Data Protection Act is primarily concerned with personal data on computers. Because it was important to clarify and update the legislation to keep pace with technology, the 1998 Act supersedes earlier legislation laid before Parliament in 1984.

It was also necessary to take account of and be consistent with the provisions of the Freedom of Information (FOI) Act, which was being formulated at the same time. The FOI Act makes some amendments to the Data Protection Act, and the Data Protection Registrar/Commissioner became the Information Commissioner responsible for both sets of legislation.

The Freedom of Information Act is very widely drawn, covering all information in whatever form, but only applicable to the public sector. On the other hand, the Data Protection Act is targeted solely at personal data held on computer or other systematic filing systems, and applies to any organisation.

For example, a local authority will have tens if not hundreds of thousands of documents, some of which will contain personal data. Individuals have the presumed right of access to all these documents with the exception of personal data.

The Act is concerned with personal data about living individuals. Data is considered personal if an individual can be identified, e.g. by name, address, email or any other uniquely distinguishing information.

There is a little-known provision covering the use of CCTV – which could be of significance to any individuals who become a subject of surveillance. Those who manage or process personal data – individuals or organisations – are defined as data controllers. As such, they have a duty to register under the Act. In fact, its provisions bind them whether registered or not.

Importantly, having data processed overseas does not exempt UK organisations.
3.2.1 The Eight Data Protection Principles

These principles provide a useful shorthand to the Data Protection Act’s scope. The data should be:

1. Processed fairly and lawfully.
2. Processed for limited specified, lawful purposes.
3. Adequate, relevant and not excessive.
4. Accurate and kept up to date.
5. Not kept for longer than is necessary.
6. Processed in line with the individual’s rights.
7. Secure from unauthorised or unlawful access and accidental loss.
8. Not transferred outside the EU to areas without adequate regulation.

3.2.2 World Wide Web

With the growth of the Internet, vastly more information is now readily available than ever before. A significant amount is personal data and it is essential for organisations that use the Web to be careful how they collect and use it. Beware. It is much easier to breach the Act than may be generally imagined!

Internet and related technology provide many ways of collecting information from a computer user. Some of these may be in subtle background mode, of which an average user could be completely unaware.

Harvesting data about or from individuals by stealth breaches the fairness principal, even if it is without malign intent. Data gatherers must be explicit and up front when collecting data. They must precisely define the purpose for which the data is being collected and with whom it may be shared.

Those who trawl for data across the Web will encounter another problem themselves and may produce even more problems for others. For example, when coming across personal information, a data gatherer may not know the terms under which that data was originally collected, or what usage was approved by the individual concerned. Mere holding of such data could be illegal – both for those who access it as well as those who placed it on the Web. The latter could be in breach of the Act in respect of a failure in their duty of care to ensure that the data is secure from unauthorised access.

3.2.3 Exemptions

There are a number of exemptions under the Act, which include national security, crime, taxation, health records, and aspects of journalism. An important exemption relates to family records, which if not present, would require one to register for one's private household records.
3.2.4 Rights and Recourse

An individual can request from an organisation the details of any information held about them and the purpose for holding the information.

Such a request has to be in writing (which includes email). The data controller is bound to respond within a reasonable time and the response has to be clear and understandable. Bodies holding such data have the right to make a modest charge to service the request and they have limited options to refuse.

An individual has the right to stop direct marketing that is reinforced by EU regulation regarding electronic communication. There is also an entitlement for individuals not to have decisions made about them by purely automated means. Anyone unable to get a satisfactory response from a data controller to resolve an issue can go to court or ask the Information Commissioner to issue an enforcement notice.

3.3 Legal Admissibility

Information is now one of the most valuable assets with an increasing amount stored electronically. It is critical that such information is properly maintained to the highest standards – that which a court of law would accept should the worst occur. The same is true when complying with regulatory authorities or resolving a dispute with a commercial partner. By adopting best practice, there can be a dramatic improvement in the validity of information accepted by the courts and others. The law changed with the Civil Evidence Act 1995. This change means that copies of documents – photocopied, filmed or electronically stored – are considered valid evidence. It is considered secondary evidence as it is not the original. There is legal precedent that it is for the courts to decide the evidential weight of such documents or how faithful a copy it is of the original.

The better an electronic document is demonstrated as a true copy of the original, the more likely it will be accepted as convincing evidence. While it is true that an original document will carry more authority than a copy, it is also the case that an original may be lost, mislaid or destroyed.

3.3.1 Principal Guidance

The principal guidance is published by the British Standards Institute in their title 'Code of Practice for legal admissibility and evidential weight of information stored electronically' (BIP 0008). It sets out five principles of good practice:

1. Recognise and understand all types of information.
2. Understand the legal issues and exercise a duty of care.
3. Identify and specify business processes and procedures.
4. Identify enabling technologies to support business processes and procedures.
5. Monitor and audit business processes and procedures.
3.3.2 Classification

A fundamental requirement is that all documents and data are identified and classified. How documents are handled, secured and potentially destroyed must be clearly defined and the procedures governing this must be agreed and authorised by senior management. Circumstances will change so it is important that procedures and relating documentation are revised.

In practice, this should be part of a more general risk analysis statement as outlined in the British Standards document ISO 17799. Previous versions of procedures need to be kept to demonstrate what was in force earlier.

3.3.3 A True Copy?

Properly categorizing information and documents can improve authenticity and evidential weight. It is also important to demonstrate that procedures are robust and properly managed. As documents go through their lifecycle, a number of operations will be performed on them or decisions taken based on their content. It is crucial that this is reflected in an audit trail as it shows the document as part of an overall and dynamic process. Metadata, or the data that describes the documents, is also relevant and should be managed with the same diligence.

The duty of care has been reinforced further with the Data Protection and Freedom of Information Acts where legal obligations now exist. One can only be confident that responsibilities are being fulfilled by undertaking a proper risk analysis that ensures all reasonable eventualities are considered. With current technology allowing documents to be stored electronically and to be backed up easily, keeping documents on paper alone is insufficient. Fire, flood, theft or malicious damage may be rare events but are real nonetheless and risk analysis should cover these possibilities.

3.3.4 Keeping Current

Over time changes occur to legislation, regulation and business practices. Precedents are set in landmark cases. Therefore guidance on best practice cannot be static. It is vital that procedures and practices are revisited on a regular basis. It is also important that there are regular audits of procedures to ensure that an organisation continues to be compliant. Following this guidance will strengthen veracity and standing when asked to demonstrate authenticity of documents and data. This is especially the case in a court of law.

To achieve this, an organisation needs to have an effective system in place. Computerised document and records management systems are designed to assist in this area. Indeed, there are now cost-effective technologies and individual solutions that have been specifically developed to address this area. These should be considered as part of an overall strategy.
3.4  Financial Regulation

Global markets with increasingly rigorous financial legislation and regulation have set higher business process standards. Now that business is truly international, UK legal compliance is no longer sufficient and other regulatory regimes must be considered. This raises the level of auditing required and, as a result, the amount of information that has to be held and accounted for. Realistically, the volume and detail of information that needs to be tracked can only be managed by the new technologies underlying the latest generation of accounting, document management, workflow and related software solutions.

It is impossible to cover the vast swathe of regulation in brief, so here are two examples of important legislation that have a significant impact across the entire spectrum of business, industry and government. They are the US-enacted Sarbanes-Oxley Act 2002 and the UK Financial Services and Markets Act 2000.

3.4.1  Sarbanes-Oxley Act

Quite often referred to as SOX or SarbOx, this legislation was enacted in the wake of a number of large, high-profile corporate failures. The Act imposes much tighter corporate governance and financial transparency. For example, there is legislation requiring executives of US corporations to demonstrate that adequate internal controls and procedures for financial reporting are in place.

A significant portion of the regulation focuses on the integrity of computer systems that underpin much corporate decision-making and disclosure to shareholders. Those covered by the Act must have methods to maintain audit trails and to log the possible altering of electronic records. Here is a short checklist of practices a company needs to implement in order to comply with SarbOx:

- Access control to monitor attempts to access the company’s financial reporting system or the data that feeds the system.
- Configuration control to monitor the configuration, policies and software installed on systems covered by the Act, and all other systems with access.
- Malicious software detection to collect and report malicious activities caused by viruses or other malicious code from a wide variety of sources – with centralised analysis.
- Policy enforcement to verify that all users are complying with regulations to reduce the chance of accidental exposure of sensitive information.
- User monitoring and management to create a complete audit of the activities of non-employees with access to private data, and take steps to minimize the risk from compromised accounts.
- Environment and transmission security involving the ongoing monitoring of the environment to ensure that security threats are detected and corrected as quickly as possible through proactive measure such as virus attack scans. Additional monitoring is required to ensure that the transmission of sensitive data is secured.
Companies have found the cost of compliance to be significant, with BP citing $18 million for its US operation. While this is purely US legislation, it impacts companies operating in the US and subsidiaries of US companies operating abroad. Many speculate that it will not be too long before the EU enacts similar legislation. No doubt the trigger will be a high profile event in a major EU country along the lines of those in the US that prompted SOX.

3.4.2 Financial Services Act

The UK Financial Services and Markets Act 2000 consolidated a fragmented regulatory position. In so doing, it created the Financial Services Authority that is primarily concerned with banking, insurance and investments. However, it has powers for most things financial.

Interestingly, the Authority is independent of government. It is financed by the industry it was set up to police. While the Treasury appoints the board, which sets overall policy, the executive makes all day-to-day decisions. However, the Authority is ultimately accountable to Parliament through the Treasury.

The Authority also has powers entrusted to it under more than half a dozen other Acts and EU directives, making it one of the most, if not the most, powerful regulator in the UK. The Authority has four statutory objects:

1. To maintain confidence in the financial system.
2. Promote public understanding of the financial system.
3. Secure the appropriate degree of protection for consumers.
4. Reduce financial crime, and reduce the extent to which it is possible for a business to be used for a purpose connected with financial crime.

As can be imagined, with such complex legislation concerned with money, the audit requirements are stringent. Record keeping has to be precise and is subject to inspection at any time.

Essentially, the financial sector is the most heavily regulated in the UK.

3.5 Technology

A wide range of advanced, specialist technologies have been developed specifically for document management. Diversity and the rapid rate of development call for a high level of competence for their successful integration and the provision of cost-effective, reliable business solutions.

Here is a brief tour through some of the main elements of these technologies. They include scanners, data storage, standards and software.
3.5.1 Scanners

Paper documents are still being generated and stored in vast quantities despite the technology available to virtually eliminate them. As a workaday medium, they can be very convenient.

However, paper has several considerations. It does not come in uniform shape, size, quality or condition. It represents a challenge to the manufacturers of scanners used to convert such material into a digital stream. There is no problem with a single page. Place it on a flatbed scanner. Close the lid and press start. But if there is a need to capture thousands of pages a day, then automated feed is required.

The first problem is the purely mechanical task of ensuring that the variations in paper can be handled and only one page is picked at a time. The second is to ensure that the quality of the image captured is an acceptable facsimile of the original, especially where the original is faded or in poor condition.

Better scanners use ultra sonic detectors to monitor and correct single page feeding. They work by sensing resonance caused by air pockets trapped between two sheets of paper. Microchip speeds are increasing all the time and the cost of processing power is falling inexorably. It is now possible to have significantly more intelligence in scanners. For example, to assist in the correction of images by automatically adjusting contrast levels and handling full colour. Such features are now becoming increasingly standard.

3.5.2 Storage

Scanned documents consume a good deal of storage with a monochrome image averaging 40k, and colour images 5 to 10 times that. In addition there is the need to ensure that documents are secure and meet the correct standards for legal admissibility. The main options are hard disk, hard disk array and CD/DVD.

The capacity of hard disks has increased rapidly and can accommodate many images. However, it is a vulnerable medium. At some point it will fail. Data can become corrupted, be too easily deleted, and is open to casual inspection. Used alone, this is the least satisfactory medium for legal purposes and needs a good backup regime to avoid loss.

A hard disk array is a configuration of hard disks arranged in such a fashion that the failure of a single disk will not result in the loss of data. These are known by a number of acronyms including RAID, SAN and NAS.

This arrangement is clearly more robust, and as it is frequently under the control of the IT department, should be more secure. Many larger organisations rely on this method of storage and, with appropriate procedures, it is better at demonstrating the legal standing of stored documents. A CD/DVD is an extremely handy and portable medium to store information. However, it is vulnerable to damage, theft, and degrades over time. As a result it is not recommended for long-term storage. If write-once media is used, then it has the merit that once burnt, it cannot be altered. This meets an important test of legal admissibility.
Should the most robust records storage technology be required, then magneto optical (MO) should be the choice. Most users will select the write-once media as it offers the highest level of integrity. It offers high capacities, particularly when configured in a jukebox, cannot be affected by magnetic forces that would destroy a hard disk, and is certified to be good for decades.

The information is written to the optical platters in the same way as on a hard disk. However, this can only happen at very high temperatures achieved by a highly focused laser beam. At lower temperatures the media is completely stable, and cannot be altered.

3.5.3 Standards

The benefits of storing documents electronically in an organised fashion are self-evident. Document distribution becomes simpler and the ability to diligently control access is made possible. Tracking and auditing of activities becomes a significant management tool. Clearly the information has to be codified, and is frequently compressed for ease of handling. It would be of little use if someone else were subsequently unable to decode that information.

Standards have become critical and many are agreed internationally. For example, those which define the format of compressed files like TIF and JPEG. Another standard is the format of structured documents such as XML. Other standards emerge once their usage becomes pervasive, such as Adobe PDF. Both ease the exchange of information between systems and remove the need for the original paper.

3.5.4 Software

The market is mature and a good deal of application software exists to manage and process documents. Most will employ the standards described above and also use techniques to secure documents.

The main application types can be broken down into several broad categories. These are records management, document management, workflow, forms processing and free/full text retrieval.

Records Management

While records are normally electronic or physical documents, they may come in a variety of formats. Some lend themselves to convenient data capture and some do not. For example, such records may be in books, clipboard pads, tickets and other formats that are not easily scanned. The process involves extensively describing and cataloguing the entity/document, including the establishment of a destruction schedule. Due to the amount of information required at each stage, these systems generally require a significant amount of resources to operate.
**Document Management**

This is generally more concerned with scanned and electronic documents, and will be indexed to the level the application demands rather than to a comprehensive schema as in a records management system. Records and document management systems frequently compete for the same customers.

**Workflow**

Workflow is the automation of tasks based upon a set of rules that will generally be part of, or supplementary to, a records or document management system. The great benefit of performing tasks in this fashion is that work can be completed in a fraction of the time it would take by other means. Properly implemented, it will offer greater control, better accountability, improve productivity, and generally pay for itself in a very short time.

**Forms Processing**

Forms processing provides a means of collecting information via a web browser or paper forms. The products are routinely used for surveys and questionnaires. People often use this technology – in many cases without realizing it. For example, by filling in warranty registrations, entering numbers on a lottery ticket or completing a census form.

**Free/Full Text Retrieval**

This provides an automated method of indexing electronic documents. The software will index each and every word in a document except common words that can be specified. The best examples of this technology are web-based search engines, such as Google©.

Scanned images can be incorporated in this index, but have to go through a process of Optical Character Recognition (OCR). The accuracy of this recognition process is almost wholly dependent on the quality of the text on the incoming scanned image, and can be a very hit-and-miss affair. It is not to be wholly relied upon. More sophisticated products will use pattern matching techniques to interpret a whole word rather than the individual characters which can overcome some of the more simplistic approaches.
4 Company Policy

4.1 What is a Document Management Policy?

All systems and documents, unless specifically excluded, are admissible in a court of law. The crucial factor is not whether a document is admissible; it is the document’s evidential weight. The evidential weight associated with any document managed by a document management system, whether electronic or not, relies on enforcing documented procedures. Enforcing a document’s evidential weight therefore relies upon companies defining and enforcing a Document Management Policy.

Defining a Document Management Policy requires the company to recognise that, first of all, it is their responsibility to define and manage their Document Management Policy and second, to clearly scope which processes and documents are to be managed by the system. The other clear responsibility for the System Integrator is to have a good working knowledge of how best to configure the system and enforce the evidential weight of the system itself and the documents managed within it. This must then be related to the client’s Document Management Policy.

Unlike ISO9000, which is more process oriented, a Document Management Policy focuses on document types, which will often cross and be used within more than one business process. The definition of a document type should be kept simple, i.e. an invoice is a document type, as is a report, a letter, and so on. Consider using the purpose of a document as a document type (for example, ‘Expense Claim’ or ‘Timesheet’), rather than application names or application types (for example ‘spreadsheet’), because these are more meaningful and easier to find.

4.1.1 Setting Up a Document Management Policy

When setting up Document Management Policy, consider the following:

- Define the scope of the Document Management Policy. This will include which documents are covered and their document lifecycle. A definition of how each document type is created and the source application or capture device is required. A definition of the process of format capture for documents is required (greyscale or black and white). The file compression that should be used also needs to be defined.

- The retention period of the document is commonly mistaken for the retention period of the media. If documents are required to be stored for 25 years, then the media must also be capable of the same period.

- A definition of access rights for user groups may also be required. In other words, a list of users’ access rights to documents and folders and drawers in the system may be required at the beginning of the project.

- A definition of how documents are to be managed in the system is also required. This also needs to include document revisions.
The destruction rules for each document are required. How are physical and electronic documents to be destroyed? When the physical document is destroyed, it is advisable to obtain and store a document destruction certificate for critical document types within the system.

Having defined the basic rules of the Document Management Policy, a more detailed definition of how each document type is to be managed is necessary. It is important to keep the Document Management Policy up to date. It is a dynamic document, which reflects changing working practices within a company, for example, the acceptance and use of fax technology a few years ago and, more recently, email.

A Document Management Policy, therefore, needs regular review. A project owner is usually responsible for managing and maintaining the policy.

Finally, and most importantly, whatever destruction policy is enforced, it is vital to inform the industry regulators of the policy, and ensure that they acknowledge the Company Document Management Policy, and give their written agreement (a document that is held as part of the Document Management Policy).

4.2 Sample Document Policy

4.2.1 Introduction

**IMPORTANT**: Disclaimer of Liability – the Sample Document Management Policy document is provided for informational purposes only. Document Logistix will not accept any responsibility for any use or misuse of the information contained herein. Document Logistix does not warrant the accuracy, reliability or timeliness of any information in this document, and shall not be held responsible for any losses caused by reliance on the accuracy, reliability or timeliness of such information.

Portions of such information may be incorrect or out of date. Any person or entity that relies on any information obtained from this document does so at his or her own risk.

This topic suggests good practices used with reference to the Document Manager Document Management System. It is intended for the use and management of documents in the Document Manager Document Management System. This document suggests practical steps that can be taken in the creation and filing of electronic documents, and basic methods for managing email messages, managing the security of shared network drives, and organising filing structures for documents.

The move towards fully electronic working methods, and the consequent need for full electronic document management, will inevitably involve many changes in approach, practices, attitudes and behaviour – for both end-users and information managers. These changes will be vital for the success of the Company as an organisation and to meet the ISO 9000 and legislative procedures.
Before proceeding, it is recommended that an internal audit is performed to assess and determine the appropriate drawer specifications to meet the business needs.

Practical developments can be achieved now to deliver rapid improvements in the quality and reliability of documents and records, for both the current business and long-term corporate memory.

Other legislative drivers, such as the Freedom of Information Act, will require all kinds of information to be recognised and managed, including both paper and electronic copies of records, even where paper files are kept conscientiously; as well as documents that may not have been classified as ‘corporate records.’

The above will only be achieved in the longer term by promoting good habits and practices within the company.

A useful model for thinking about the best point to apply good practice is referred to throughout this section:

- Corporate workspace: Contains formal corporate documents that are shared across all, or a significant part, of the organisation.
- Workgroup workspace: Contains operational documents in use by a work team, and which are shared at least between that team.
- Personal workspace: Contains documents that are only of interest to the individual.

It is suggested that any document used in workflow or communication between individuals and external clients (i.e. Suppliers and Customers) is saved into the Document Manager System. These include application documents or scanned documents.

The company’s Document Policy should cover:

- Naming conventions for documents and folders
- Document types, templates and formats
- Managing documents and access to storage locations
- User/group access rights within Document Manager
- Document Manager drawer filing structures

### 4.2.2 Software Environment

It is recommended that the software environment is stated in the Document Policy. For example:

‘This document assumes use of Microsoft® Office XP/Windows 2000/Windows XP/ Microsoft® Exchange 2003 operating environments, in particular those environments relating to the management of electronic documents including HTML, as in Websites.’
4.2.3 Document Creation and Naming Conventions

Naming conventions are standard rules to be applied to documents, and to electronic folders that contain these documents, in order to enforce consistency in the name format and in the words and phrases used. Essentially, naming conventions have two related functions:

- Bringing related items together under a common label – such as for a folder or set of documents.
- Distinguishing similar items by naming in a consistent, logical and predictable way.

For example, the term ‘folder’ refers to the Document Manager folder and items held within folders are ‘documents.’

The value of naming conventions lies in the few simple rules that take away the burden of decision and encourage consistent practice. Naming rules should follow the same logic and consistency across different types of items, following the same pattern for similar situations so that once learned, the user can reasonably predict how it will apply in a new situation.

When profiling a document in any drawer, try and be consistent in the naming convention for the document description and avoid using dynamic dates and linked documents.

4.2.4 Document Versions

In general, document versions must be controlled via Document Manager rather than relying solely on the description of the document as a version.

Use of Document Manager version control will ease management overhead immensely and the potential for conflict with later applications will be minimized. Two types of version control can be used and the use of these needs careful consideration. If the document will not be changed frequently, use the major version control (i.e. 1, 2, and 3). If documents are going through many changes, use the minor version control (i.e. 1.1, 1.2, and 1.3).

4.2.5 Document Types, Profiles and Templates

Document types should have meaningful descriptions rather than cryptic names. Use standard terms for document types such as ‘agenda’, ‘report’, ‘letter’, ‘project schedule’, ‘minutes’, ‘internal memo’, and so on.

Do not use initial terms such as ‘Power Point Presentation.PPT’ in a title because physical types such as a PowerPoint presentation are already held as an extension (.ppt) in the actual file format.

It is suggested that you do not use the document creator’s name in the title – a signed letter, for example, will give this information in the content or index field if applicable.

Document types in the Document Manager system will be restricted to particular drawers. New document types can only be created by the Document Manager System Administrator and requests for new types will have to be submitted to the line manager for further action.
Application document types defined in Document Manager will have templates where applicable.

It is recommended that you do not use the Document Properties dialog box for metadata in Microsoft® Office Word documents to profile the documents, but instead use the Document Manager document index fields.

There is the potential for misleading metadata when document production is shared, for example, where the ‘Author’ field takes the last named editor, but the ‘Organisation’ field remains the same.

It is suggested that you use standard design templates for very common document types, such as Expenses Forms and Holiday Request Forms.

Avoid using dynamic dates and linked documents within an application document. Instead, use object embedding if necessary.

For example, In Microsoft Office Word, if a dynamic date field is used in a letter, every time that document is opened, the current date is inserted automatically into the document. This is useless if the original date of the letter is to be tracked.

Decisions on when to use standard settings, and which to use, should be based on a balance between:

- Keeping it simple: Too much complexity will confuse and alienate the end user, and lead to potential misinformation.
- Keeping it useful: Only those standard settings that have a demonstrable value should be used.
- Keeping it flexible: When it is hard to anticipate all valid variations, it is usually better to adopt a minimal approach that can be modified case-by-case.

The use of standard templates for application document types, such as letters, memos, requests and reports, will:

- Ensure a greater level of consistency in document (and record) production.
- Enable documents that should be kept as corporate records to be more readily identified.
- Support a closer integration of document production with day-to-day business operations.

It is suggested that any new templates used in Document Manager have at least a footer section consisting of the document or form name and its unique reference number and version.

### 4.2.6 Storage and Distribution Formats

When more than one version of a particular software application is in use, the physical format in which documents are saved should be defined. It is always preferable to limit the number of formats as much as possible, so that current access and future migration problems are reduced.

Think about which document types will be internal and which will be external. This helps to set up the storage and distribution formats.
The basic options are:

- **Standardise on a single application version when one is in use across the whole organisation to provide complete access.** For example, use Microsoft Office Word 2010 to save all documents in the current file extension format. Legacy documents will probably need to be migrated to a future application version at some point.

- **Standardise on an exchange format, when multiple application versions are in use between two different parties or companies.** For example, use the Microsoft version of word-processor documents, by saving all corporate documents in a .doc or .docx format.

- **Standardise on a distribution format, where documents are finalised and will not be changed in content.** Use a PDF rendition, which has the advantage of making documents effectively read-only, but requires the necessary software to produce the rendition, for example, Adobe® Acrobat® (PDF readers are available freely on the Internet). Any documents distributed externally should be rendered in PDF format.

- **Standardise on an Internet format, where an intranet is the main distribution channel, supported by good document control facilities.** For example, an HTML format makes the documents very widely accessible through a standard Web browser.

Documents that are distributed to external clients should be scanned (if signed) and stored in PDF format (for example, using Adobe Acrobat).

Do not forget to include a policy around the storage of Audit Logs. Audit Logs are also considered part of the evidential weight of all documents managed by Document Manager.

### 4.2.7 Document Types Restricted to a Drawer

Users will have access to the drawers they work with and the relevant line manager should provide access to these drawers. The Document Types shown in bold below indicate that the document type should be encrypted.

Table 1 shows a few example drawers and their Document Types:

<table>
<thead>
<tr>
<th>Drawer Name</th>
<th>Document Type</th>
<th>Storage Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounts Payable</td>
<td>Purchase Order</td>
<td>Finance</td>
</tr>
<tr>
<td></td>
<td>Invoice</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Check copy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Quotation</td>
<td></td>
</tr>
</tbody>
</table>
21

Company Policy

Guide to Document Management

<table>
<thead>
<tr>
<th>Drawer Name</th>
<th>Document Type</th>
<th>Storage Location</th>
</tr>
</thead>
</table>
| Human Resources | Sickness Form
Disciplinary Warning
Birth Certificate
Death Certificate
CV (Résumé)
Performance/Salary Review
Maternity Leave form
Doctors Note
Medical Insurance
Pension | Personnel |
| Insurance     | Form
Renewal
Schedule
Invoice
Remittance Advice
Credit
Claim | Default |

Table 1: Document Types and Storage Locations for Example Drawers

### 4.2.8 Drawer Structures

Ensure the drawer structure is documented in the Document Management Policy. Over the years, this section is likely to be updated the most.

**Example Drawer Structure for ‘Human Resources’**

<table>
<thead>
<tr>
<th>Index Type</th>
<th>Index</th>
<th>Data Type</th>
<th>Field Length</th>
<th>Required?</th>
<th>Unique?</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Folder</td>
<td>Employee#</td>
<td>Numeric</td>
<td>10</td>
<td>Y</td>
<td>Y</td>
<td>1234567890</td>
</tr>
<tr>
<td>Folder</td>
<td>Last name</td>
<td>Character</td>
<td>35</td>
<td>Y</td>
<td></td>
<td>Smith</td>
</tr>
<tr>
<td>Folder</td>
<td>First Name</td>
<td>Character</td>
<td>50</td>
<td>Y</td>
<td></td>
<td>Joe</td>
</tr>
<tr>
<td>Folder</td>
<td>Start Date</td>
<td>Date</td>
<td>8</td>
<td>Y</td>
<td></td>
<td>12/1/2000</td>
</tr>
<tr>
<td>Folder</td>
<td>Status</td>
<td>Domain</td>
<td>9</td>
<td>Y</td>
<td></td>
<td>Active</td>
</tr>
<tr>
<td>Document</td>
<td>Doc. Date</td>
<td>Date</td>
<td>8</td>
<td>Y</td>
<td></td>
<td>12/1/2000</td>
</tr>
</tbody>
</table>

Table 2: Example ‘Human Resources’ Drawer Structure
**NOTE:** It is a good idea to ensure that the document types for the Human Resources drawer are on a secure server, encrypted and that only the Board and Human Resources group have access to the drawer and storage locations. Additionally, set it up so that document types such as ‘Disciplinary’, ‘Confidential’ and ‘Warning’ use a hidden storage location only accessible by the appropriate staff.

**Example Drawer Structure for ‘Insurance’**

<table>
<thead>
<tr>
<th>Index Type</th>
<th>Folder Index</th>
<th>Data Type</th>
<th>Field Length</th>
<th>Required?</th>
<th>Unique?</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Folder</td>
<td>Client Name</td>
<td>Character</td>
<td>50</td>
<td>Y</td>
<td>Y</td>
<td>Smith; Document Logistix Ltd</td>
</tr>
<tr>
<td>Folder</td>
<td>Policy Number</td>
<td>Numeric</td>
<td>10</td>
<td>Y</td>
<td></td>
<td>1234567890</td>
</tr>
<tr>
<td>Folder</td>
<td>Policy Type</td>
<td>Domain</td>
<td>N/A</td>
<td>Y</td>
<td></td>
<td>Motor, House, Life</td>
</tr>
<tr>
<td>Document</td>
<td>Doc. Date</td>
<td>Date</td>
<td>8</td>
<td>Y</td>
<td></td>
<td>12/1/2008</td>
</tr>
</tbody>
</table>

Table 3: Example ‘Insurance’ Drawer Structure

4.2.9 **Drawer-Specific Document Types**

Drawers in Document Manager can be restricted to new document types but not enforced, so users will be able to search on ‘old’ document types. Determine whether this restriction will be enforced.

For example, there is a Sales drawer set up and it has Invoice and Quotation document types. If the document type restriction is enforced, any user creating a new document in the Sales drawer can only choose the Invoice or Quotation document type. If the drawer’s document types are not enforced, a button with a plus (+) symbol appears besides the Document Type field in Document Manager. When a user clicks on that button, all the document types available in Document Manager will display for the user to choose from.

**NOTE:** For sample group and user document access permissions, refer to 4.2.14 Sample Permissions for Users and Groups on page 27.

It is a good idea to establish that any requests for the creation of new document types or changes to drawers in Document Manager are forwarded to the Document Manager System Administrator.

4.2.10 **Document Types with Regard to Emails**

Email messages can constitute part of the formal documentation of a transaction. All members of staff are responsible for identifying and managing email messages that constitute a record of their work. When an email is sent or received, a decision needs to be made by the individual about whether the email needs to be captured as a record in Document Manager. Once an email
message has been captured as a record, it should be deleted from the email client (i.e. Microsoft® Office Outlook®). The main points to consider when managing email records are:

- Identifying email records
- Who is responsible for capturing email records
- Email messages with attachments
- Where to capture email records
- When to capture email records

**Identifying Email Records**

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

When deciding whether an email message constitutes a record, the context and content of the email message needs to be considered. A guiding principle on identifying email records might be that as soon as the email message needs to be forwarded for informational purposes, it should be considered a record.

Email messages that might constitute a record are likely to contain information relating to business transactions that have taken place or are going to take place, decisions taken in relation to a business transaction or any discussion that took place in relation to the transaction. For example, during the decision to put out a request-for-information document for a particular service, background discussion about what this should and should not include might take place via email and should be captured as documents in Document Manager.

**Who is Responsible?**

Because email messages can be sent to multiple recipients, there are specific guidelines to indicate who is responsible for capturing an email as a record into a Document Manager drawer:

- For internal email messages, the sender or initiator of an email message, or dialogue that forms a series of email messages
- For messages sent externally, the sender of the email message
- For external messages received by one person, the recipient
- For external messages received by more than one person, the person responsible for the area of work relating to the message. If this is not clear, it may be necessary to clarify who this is with the other people who have received the message.
Designate a specific drawer to use for archiving non-external business-related emails. Note that any emails saved in Document Manager must then be deleted from the email client because this would duplicate storage.

- Email messages with attachments: If an email message has an attachment, a decision needs to be made as to whether the email message, the attachment or both should be kept as a record. The decision on whether an email and/or its attachment constitute a document depends on the context within which they were received. It is likely that in most circumstances the email will be captured as a document with the attachment.

- Where to capture: Email messages that constitute business records must be saved into Document Manager in the original email format. Email messages captured as documents should be located with other documents relating to the same business activity, e.g. Sales quotations sent by email should be saved into a Document Manager ‘Sales’ drawer.

**NOTE:** Personal mailboxes should not be used for long-term storage of email messages. Personal mailboxes should be used for personal information or short-term reference purposes; when these emails are no longer required, they should be deleted.

**Example Rules for Addressing Email Messages**

Limit main recipients to those who are expected to take action or decisions based on the message content.

- Add C.c. recipients for information only.
- Use the ‘Reply to all’ function with care, balancing open communication against message overload – consider the recipient.
- Avoid sending global messages to all users – post a global message on a Company Forum.
- Consider whether email is the appropriate channel to communicate this message.

**Examples Rules for Managing Emails**

Below is a list of sample rules for managing emails in the company:

- Use clear and descriptive subject lines.
- Indicate if no reply is needed.
- Do not resend attachments with a reply unless necessary.
- Resist the tendency to drift away from the precise topic of a thread of discussion by introducing material on an unrelated topic.
- Do not bundle together several topics in one email. It is better to create separate messages for separate topics, in the same way that a text document should have a single central focus.
• As a business rule, use the ‘Reply with original text’ feature, enabled in the email client. The final email sent will need to be archived in Document Manager.

• Do not reply by annotating the original text at various points – it is better to group all replied text together in one place.

• Do not embed earlier email messages within the current email message because this makes it difficult to manage emails and leads to confusion.

**When to Capture Emails and Responsibilities**

For the saving of emails, determine whose responsibility it is to save emails received into Document Manager. Below is a list of examples:

- For emails related to Customer Support (including complaints), it will be the Helpdesk person.
- Finance-related emails will be the Office Manager.
- Marketing-related information will be the Marketing Manager.
- Corporate-related information will be the Operations Director.
- Training-related emails will be the Training/Publications person.

**4.2.11 Disposal of Documents and Document Retention Periods**

In all cases, ‘good housekeeping’ of both shared and personal documents is essential in maintaining long-term viability, and in removing material that should no longer be kept (whether classed as ‘document’ or ‘record.’) Since good management in this environment depends largely on the Document Management system, some duplication (by document reference) and redundancy will probably be necessary to ensure good access for business purposes.

Below are some example rules in regard to document retention:

- Users of Document Manager should manage their own documents by using the ‘Check Out/Check In’ and ‘Version Control’ features for application documents.
- To comply with the Data Protection Act, documents such as CVs/résumés of persons who have been interviewed and not offered a job should be deleted by the Human Resources department after 28 days from the date a notification letter was sent.
- More details regarding document retention periods with reference to document types are discussed in **4.2.15 Sample Document Retention Periods** on page 30.
4.2.12 Physical Storage Locations and Secure Shared Drives

In order to improve security, the physical shared locations on the server should have restricted access based on user access permissions.

A Windows-shared secure drive used in conjunction with Document Manager will offer a good security model.

**Sensitive Information**

The shared drive areas where classified documents are physically stored will be encrypted to provide high security and the shared drive should also be restricted to authorised Document Manager users.

4.2.13 Groups and Users

An integral part of the Company Document Management Policy is to have a list of groups and users and their access rights and permissions. Document Manager allows the setup of the groups and users in a fashion similar to the company organisation chart. An example company organisation chart is shown in Figure 1:

![Example Company Organisation Chart](image)

*Figure 1: Example Company Organisation Chart*
### 4.2.14 Sample Permissions for Users and Groups

**Drawer Name ‘ACCOUNTS PAYABLE’**

<table>
<thead>
<tr>
<th>Permission Type</th>
<th>Permission</th>
<th>Group Name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Finance</td>
</tr>
<tr>
<td><strong>Document</strong></td>
<td>Allow External Reference</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Check Out</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Copy</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Copy Reference</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Create</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Delete</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>E-Mail</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Export</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Modify</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Modify Access</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Move</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Open</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Open MetaData</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Print</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Set Read-Only</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Set Read-Write</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Undo Any Check Out</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>View</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>View Audit</td>
<td>X</td>
</tr>
<tr>
<td><strong>Folder</strong></td>
<td>Create</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Delete</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Modify</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Modify Access</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>View</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>View Audit</td>
<td>X</td>
</tr>
<tr>
<td>Permission Type</td>
<td>Permission</td>
<td>Finance</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Annotations</td>
<td>Append Sticky Note</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Apply Image Stamp</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Create Drawing Object</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Create Image Stamp</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Create Protractor</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Create Redaction</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Create Ruler</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Create Sticky Note</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Create Text Stamp</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Create Typed Text</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Delete</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Hide Redaction</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Modify Access</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Modify Properties</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Modify Sticky Note Text</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Move/Resize</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>View Drawing Object</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>View Protractor</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>View Ruler</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>View Sticky Note</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>View Text Stamp</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>View Typed Text</td>
<td>X</td>
</tr>
<tr>
<td>Batch</td>
<td>Admin</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Create</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Delete</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Exceptions</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Index</td>
<td></td>
</tr>
<tr>
<td>Permission Type</td>
<td>Permission</td>
<td>Group Name</td>
</tr>
<tr>
<td>-----------------</td>
<td>----------------</td>
<td>-----------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Finance</td>
</tr>
<tr>
<td>ScreenScrape</td>
<td>Create</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Delete</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Modify</td>
<td>X</td>
</tr>
<tr>
<td>Administer</td>
<td>Global Access</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Super Administrator</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Administer Audit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Administer Databases</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Administer DocTypes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Administer Domains</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Administer Drawers</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Administer Groups</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Administer Selected Drawers</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Administer Selected Groups</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Administer Storage Locations</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Administer System Settings</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Administer Text Stamp Values</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Administer Users</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Administer Workflow</td>
<td></td>
</tr>
<tr>
<td>Misc</td>
<td>Can login to Desktop/Rich Client</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Can login to Web/Internet</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Can login to Web/Intranet</td>
<td></td>
</tr>
</tbody>
</table>
### Table 4: Sample Users and Group Permissions for ‘Accounts Payable’ Drawer

<table>
<thead>
<tr>
<th>Permission Type</th>
<th>Permission</th>
<th>Finance</th>
<th>Marketing</th>
<th>Senior Managers</th>
<th>Human Resources</th>
<th>System Admin</th>
</tr>
</thead>
<tbody>
<tr>
<td>Misc (continued)</td>
<td>Export Search Results on Web</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Make all fields available on Web</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td></td>
<td>Never disable after incorrect password</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

Table 4: Sample Users and Group Permissions for ‘Accounts Payable’ Drawer

### 4.2.15 Sample Document Retention Periods

Depending on the industry, document retention periods will vary. Consult with industry regulators and get a copy of the requirements for retaining documents. Do not forget to take into account explicit provisions for any confidentiality agreements that may affect the organisation.

Table 5 shows sample retention periods for different aspects of business (CFY = current fiscal year):

<table>
<thead>
<tr>
<th>Business Aspect</th>
<th>Description</th>
<th>Retention Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finance</td>
<td>Financial Forecasts and Budgetary Working Papers</td>
<td>CFY + 6 years</td>
</tr>
<tr>
<td></td>
<td>Final Estimates</td>
<td>Permanently</td>
</tr>
<tr>
<td></td>
<td>Financial Strategy – 5 year plan</td>
<td>Permanently</td>
</tr>
<tr>
<td>Financial Reporting</td>
<td>Closing papers and notes related to year-end accounts</td>
<td>CFY + 10 years</td>
</tr>
<tr>
<td></td>
<td>Financial statement, details accounts, tax returns</td>
<td>Permanently</td>
</tr>
<tr>
<td>Ordering</td>
<td>Tendering documentation (invitations, bids, evaluations, etc.)</td>
<td>CFY + 6 years</td>
</tr>
<tr>
<td></td>
<td>Official Orders</td>
<td>CFY + 6 years</td>
</tr>
<tr>
<td></td>
<td>Delivery Notes, Goods Received Notes</td>
<td>CFY + 6 years</td>
</tr>
<tr>
<td>Purchasing</td>
<td>Purchase Invoices, Credit Notes, including Expense Claims, petty cash floats, etc.</td>
<td>CFY + 6 years</td>
</tr>
<tr>
<td></td>
<td>Check authorisation reports</td>
<td>CFY + 6 years</td>
</tr>
<tr>
<td></td>
<td>BACS Reports</td>
<td>CFY + 6 years</td>
</tr>
<tr>
<td></td>
<td>Management of relationship with suppliers.</td>
<td>Termination dates + 2 years</td>
</tr>
</tbody>
</table>

NOTE: Retain transaction information in archive form for a further 4 years after deletion.
<table>
<thead>
<tr>
<th>Business Aspect</th>
<th>Description</th>
<th>Retention Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>Human Resources</td>
<td>Individual Staff files</td>
<td>Date of leaving + 10 years</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> Summary information of employment to be held indefinitely, e.g. name, DOB, department, salary, pension scheme, basic payroll record, etc.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Staff Redundancy Records &lt;20</td>
<td>Redundancy date + 3 years</td>
</tr>
<tr>
<td></td>
<td>Staff Redundancy Records &gt;20</td>
<td>Redundancy Date + 12 years</td>
</tr>
<tr>
<td></td>
<td>Organisational Development: Staffing Structures</td>
<td>Permanently</td>
</tr>
<tr>
<td></td>
<td>Staff Performance Appraisal Reports</td>
<td>6 years from end of employment</td>
</tr>
<tr>
<td></td>
<td>Application forms/interview notes</td>
<td>Interview date + 1 year</td>
</tr>
<tr>
<td>Estate Management</td>
<td>Legal Aspects of Ownership – Deeds, Licenses, Leases, Planning Applications, etc.</td>
<td>Permanently</td>
</tr>
<tr>
<td></td>
<td>Administration of Properties, etc.</td>
<td>Disposal + 10 years</td>
</tr>
</tbody>
</table>

Table 5: Sample Document Retention Periods
# Index

## C
- Company Document Management Policy ......................... 15
- Contact Details ...................................................................... i
- Conventions in Use ................................................................ 1

## D
- Data Protection Act................................................................. 6
- Document Management
  - Company Policy .......................................................... 15
  - Document Conventions .................................................. 18
  - Document Disposal......................................................... 25
  - Document Types for Emails ........................................... 22
  - Document Types, Profiles and Templates ....................... 18
  - Document Versions ....................................................... 18
  - Drawer Structures.......................................................... 21
  - Group and User Access and Permissions ....................... 26
  - Overview........................................................................ 3
  - Physical Storage Locations ............................................. 26
  - Restricted Document Types ......................................... 20
  - Sample Document Policy ............................................. 16
  - Sample Document Retention Periods ............................. 30
  - Setting Up a Policy ........................................................ 15
  - Software Environment ................................................ 17
  - Storage and Distribution Formats ................................. 19
  - What is a Document Management Policy? ..................... 15

## F
- Financial Regulation ............................................................ 10

## L
- Legal Admissibility.............................................................. 8

## M
- Manual Conventions .......................................................... 1

## O
- Overview........................................................................... 3

## S
- Sample Document Policy .................................................. 16
- Sarbanes-Oxley Act .......................................................... 10
- Setting Up a Document Management Policy ................... 15
- Support............................................................................ i

## T
- Table of Contents ............................................................... iii
- Technology ....................................................................... 11

## W
- What is a Document Management Policy? ....................... 15