PUBLIC
RECORD
OFFICE
The National Archives

Good practice in managing electronic documents

using Office 97 on a local area network

Contents

Section One : What is the purpose of this toolkit?

1 : Summary introduction

This toolkit describes good practice for the management of electronic documents in an operating environment typical of many government departments and agencies – using the MS Office 95/97 application suite and MS Exchange/Outlook on a Local Area Network – with organisation-wide e-mail and shared network drives, but without the assistance of any more specialised document or records management software.

It is not a substitute for full electronic and document records management (EDRM). It should be used to prepare for full EDRM by introducing guidance, rules and procedures for the creation, organisation and sharing of electronic documents which may or may not be printed and filed as formal records. The toolkit asks the question: "*What can we start doing now to improve current practice?*" and proposes some answers as a good first step in the transition.

1.1 : The problem

- Staff are using office software and e-mail to create and exchange electronic documents; but the organisation is attempting to manage these documents as corporate records in a paper format, with a general 'print to paper' policy for any document or e-mail which relates to departmental business.
- Unfortunately, on the one hand, documents are often not actually printed and placed on a paper file, because this is seen as increasingly burdensome by the end user at the desktop.
- On the other hand, the electronic version of the document is not consistently managed either; documents may be stored unpredictably in a variety of locations and under varying names, and with no guarantee of lasting access or accuracy.

1.2 : Best practice

The toolkit suggests some areas where good practice can be developed, but it is not completely prescriptive in defining what these should be. A particular operating environment, established ways of working, and other factors, will influence decisions on those areas that are the most important to address, and those where practical outcomes can actually be achieved, in any specific department or agency. The toolkit is intended for the records or information manager to use in developing a statement of best practice for their own organisation; it is not in itself a statement of best practice that can be passed directly on to end users.

1.3 : Summary of contents

Section 1 covers:

- the nature and purpose of this toolkit
- the reasons why action is worthwhile

- the audience, scope and outcomes
- the relationship to the 2004 target.

Section 2 covers:

- practical steps that can be taken in influencing the creation and filing of electronic documents
- basic methods for managing e-mail messages
- shared network drives
- organised filing structures for electronic material.

Section 3 covers:

- stakeholders that will need to be consulted in taking this approach forward
- prioritising the parts of the organisation to tackle first
- developing commitment and expertise at the local level.

1.4 : Relation to 2004

This toolkit supports achievement of those milestones given in the 2004 route map which deal with issues of bringing existing electronic documents and records under managed control. It aims to:

- provide mechanisms for the better management of existing material identified as important by the inventory and appraisal strategy
- help feed information into the strategic plan and detailed requirements for corporate electronic records management
- map out links with paper records that will be needed in constructing an electronic fileplan
- help determine appropriate policy and guidance for electronic document and records management (EDRM)
- support and encourage changes in end users habits, practices, and understanding that any successful EDRM implementation will require.

1.5 : Is it worth the effort to do this now?

The move towards fully integrated electronic working methods, and the consequent need for fully integrated electronic records management, will inevitably involve many changes in approach, practices, attitudes and behaviour – for both end users and for records and information managers – that will be vital for success. One simple answer to the question '*Why is it worth bothering with all this now?*" is that these changes will have to take place in any case, in the longer term; and it is better to start the process early and in a controlled manner than to be forced by circumstance.

The case For

- Practical developments can be achieved now to deliver rapid improvements in the quality and reliability of documents and records, for both current business and long-term corporate memory.
- A business case for electronic records management can be developed from a practical base, and within the context of document and information management.
- The profile of records managers within the organisation as the responsible role for delivering those benefits can be made explicit.
- Other legislative drivers, such as Freedom of Information, 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.

These will only be achieved in the longer term by promoting good habits and practices in the end user community.

The case Against

- Improving local conditions for information and record access may be detrimental to the achievement of organisation-wide records management in the long term by making the move from local to corporate control appear to offer less ‘value for money’ once there is an evident improvement at the local level.
- A direct move from little or no control to corporate level electronic records management may seem more attractive.
- The introduction of intermediate stages that are not carefully thought out may introduce extra complexities for migration of records and procedures, and confuse the end user in the long term.

The extent to which an individual organisation will draw on the proposals in this toolkit will depend on its own situation, relationships with other electronic initiatives, and its strategy for achieving 2004, for example where good practices are being introduced:

- in preparation for an already identified solution
- where a longer-term solution is not yet identified

In general, the current recommended good practice for major projects in a government IT environment is to take a modular and/or incremental approach wherever possible, to improve control and lower project risk.

The key point is to recognise that the transition to full electronic document and records management is a wider programme which must start from the situation the organisation is currently in, and is more than the implementation of a piece of software. This toolkit describes one approach which can be taken in the early part of that transition.

2 : Purpose and scope

This toolkit supports the achievement of the 2004 target by focusing on actions and activities that can be initiated now – prior to the implementation of full EDRM systems, software and procedures.

The toolkit aims to support two general purposes:

- developing good habits and user practices in the creation and organisation of documents, as a platform for the introduction of more formal document and record management software in the medium term
- taking initial steps in the development of electronic records management control, working from a base within the current information architecture.

2.1 : Aims and intended use

The toolkit identifies common ground between records management and information management – areas where relatively minor developments in practice and procedures can benefit both. Good practice in managing information, at the personal, workgroup and corporate level, will support good records management, and vice versa. Toolkit users should identify those areas in which smaller changes can be leveraged to greater overall benefit. The toolkit is not intended to be completely prescriptive, and it is certainly possible to put into practice some but not all of the measures described. It is more important to be clear, cogent and consistent in promoting good practice to end users than to be completely comprehensive.

Over time, the toolkit will be supported by examples and case studies of challenges and successes in actual practice, both through the medium of RM Forum (the Community of Practice for government record managers) and by other publications from the Public Record Office. In addition, the toolkit itself will be updated to reflect this growing practical knowledge from time to time.

2.1.1 : Audience

The toolkit is primarily addressed to records managers in government and to others, such as information managers or IT managers, who have records management responsibilities. It assumes a reasonable level of general IT and information literacy, including a broad familiarity with standard office software and an e-mail client; it does not assume a specialist IT knowledge or familiarity with 'back office' software.

2.2 : Software environment

The toolkit assumes use of MS Office 95 or MS Office 97 office application suite, and MS Exchange client or MS Outlook 97/98 for e-mail messaging, running under Windows 95/98 or Windows NT4. The specific examples given may not always be transferable to other software environments.

This toolkit does not cover the additional issues stemming from use of MS Office 2000 / Windows 2000 / Exchange 2000 operating environment, in particular those relating to the management of electronic documents and records in Intranets and Websites – this will be addressed in a separate publication.

Electronic documents and records

Many electronic ***documents*** are produced in the course of departmental business, with varying degrees of value and longevity. These can be in various versions – working documents, draft documents, finalised documents – and formats: conventional text-based documents, e-mail messages taking the place of memos or phone calls, e-mails commenting on attached text documents; spreadsheets, multimedia documents, linked and embedded documents. In this toolkit, the term 'document' refers to any digital object commonly found in office systems: spreadsheets, word processed files, discrete databases, and presentations are examples.

Not all documents will acquire the status of formal ***records***, but it is of course important to ensure those that should do, do so and are managed as such. In practice, there is not always a clear distinction made between ***electronic documents*** and ***electronic records***, because of a growing gap between record-creating and record-keeping technologies. As people become more used to working electronically, the gap between the documents which a user creates and the records which are managed widens: because users do not 'print and file' documents systematically: because of the difficulty of printing some types; because they mean to but forget; because they are inconsistent, and so on.

This toolkit is aimed at those electronic documents which are more formal and that would be expected to be kept as records in one form or another, narrowing the gap by better management of all these documents whether declared as a formal record copy or not. Some may have a paper equivalent, some perhaps should have but do not. In the medium term, we will expect to manage all this material in electronic form in any case.

2.3 : Toolkit products

There are three main products which can be produced from this toolkit:

- guidance on best practice in managing electronic documents, for end users
- contribution to plans for moving to full electronic records management across the organisation
- contribution to a strategy for culture change, moving towards thinking and working electronically.

2.3.1 : Guidance on best practice for users

The toolkit is for use in producing guidance for end users. This should be expressed in the terms understandable in a familiar work environment, and provide concise, practical and clear procedures to follow, aiming to help users easily to identify the right actions to be taken in commonly recognised situations. It should set out roles and responsibilities in terms which can be understood by, and are meaningful to, the end user.

All best practice documentation must be consistent with all relevant corporate policy documents, particularly the corporate policy on electronic records. It is particularly important that any 'print to paper' policy is clear and unambiguous; changes to this policy should establish precise conditions for its operation.

2.3.2 : Preparation for full ERM system

This toolkit will assist planning the introduction of full electronic records management by 2004 by:

- using the inventory of electronic record collections to identify and prioritise collections that should be brought into a more managed environment using methods from this toolkit
- developing document collections which may be candidates for migration into a managed ERMS, or which at least provide compatible legacy data
- supporting an analysis of the structure and nature of documents that are actually being produced in the electronic environment, rather than those typically produced in a paper environment
- feeding into the strategic planning for EDRM, guiding decisions on implementation such as: which areas to address first, which are most receptive, and which give the best examples to follow?

2.3.3 : Contribution to cultural change

Practical application of the steps set out in Section 2 of this toolkit have potential for enabling the cultural change process by:

- initiating or strengthening change in habits and perceptions in the end user population
- encouraging the sharing of documents, and demonstrating the value-added and business benefits of high quality corporate level information
- demonstrating to the individual the value of better personal organisation in creating and capturing documents and records
- supporting the convergence of electronic records management with information and knowledge management systems.

Section Two : What practical steps can be taken?

Section summary

This section deals with some specific steps towards good practice that can be developed within the typical local network / shared drive environment assumed by this toolkit. While the specific practices that are appropriate for any particular organisation will vary, and will themselves develop and extend over time, the general principles are constant. The aim is to establish practices which support a better corporate organisation of electronic documents and records, *and* which the end user will find helpful in organising their own work and their interaction with documents produced by others.

In deciding which methods to introduce to the organisation, identify and consider steps which:

- are consistent with the strategy for introducing electronic records management, and which prepare the ground for this
- will be most successful in achieving rapid results, and which work well together to greater overall effect
- will build commitment from end users and business managers.

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

- corporate workspace, which contains formal corporate documents that are shared across all, or a significant part, of the organisation
- workgroup workspace, which contains operational documents in use by a workteam, and which are shared at least between that team
- personal workspace, which contains documents that are (at present) only of interest to the individual.

A document – for example, a text document or e-mail – will usually move between different workspaces during its lifecycle.

This section covers :

- naming conventions for documents and folders
- document metadata, templates and formats
- managing e-mail
- shared network drives
- building corporate filing structures

3 : Naming conventions : documents and folders

Summary : naming conventions

- at a basic level, use standard forms of names and avoid redundancy
- develop standard ways of ordering elements in more complex titles
- establish standard ways to identify document versions
- apply consistent conventions to both document and folder titles
- keep conventions as simple as possible and easy to use

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 form of name 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.

In the context of this document, the term *folder* refers to a Windows operating system folder unless otherwise specified.

Rules for naming documents and folders should be kept simple and clear, so that they can easily be introduced and followed. It is preferable to compromise on a broader approach that can be clearly understood and remembered, than a more detailed and sophisticated structure that is less likely to be used in actual practice.

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.

Conventions for naming electronic documents should be co-ordinated with those for naming folders, so that a document title does not contain unnecessary general information already present in the folder in which it is filed: for example the name of a project or organisational division.

3.1 : Standard terms

Standard terms and forms of name should be used wherever it is sensible to do so. In particular, this can apply to:

- names of organisations and people
- names of projects and activities
- logical document types.

At this basic level, names should consist of sensible, short phrases. Proper names should always use *either* the full form of the name *or* the acronym.

Example of rules for standard name forms

- use GSI not Government Secure Intranet, *or*
- use Government Secure Intranet not GSI
- use e-government not electronic government
- use standard common terms across units, such as: *budgets*; *progress report*

Logical document types should also use standard terms. It is usually not necessary to repeat information in the document title which is already available from the directory display. The physical form of a document is held in the file extension, or displayed as a directory icon, and the date of creation/modification is also available.

Example of rules for standard terms for document types

- use these standard terms for: agenda; report; letter; project schedule; minutes
- do not use initial terms such as *Presentation on …* in a title because physical types such as a PowerPoint presentation are already held as .ppt in the directory display
- do not use the document creator's name in the title – a signed letter, for example, will give this information in the content.

3.2 : Structured titles

The naming convention approach can be developed into a more detailed structuring system for the individual elements of document titles. The general principle is to identify the logical aspects of a document type, and to list these in the most effective order for access, rather than to use a looser 'narrative' form.

Examples are:

Examples of structured titles for documents

- consistently structure personal names in *surname, forename* order
- arrange **document** titles which reflect organisational structure in reverse hierarchical order (most specific first) as in *Training Unit* : *Personnel*, but do not repeat elements already in the **folder** title in which the document will be filed
- where a date is necessary in the document or folder title, order the elements so that they display chronologically, for example in a *YYYYMMDD* pattern; months spelled alphabetically do not file in chronological order
- for standard document types, combine elements of a title to give the most useful information first, bearing in mind the folder structure and titling; for example, for a letter: *topic – recipient – letter type.*

Document titles should contain enough information to identify them if they become detached from the correct folder – a large number of documents entitled *2000-04 Minutes* is not helpful. Naming conventions should aim to strike the right balance between:

- *brevity*: keeping titles short; and *usability*: usefully describing the content

- *specificity*: using very precise terms; and *collocation*: grouping under broad headings

that will assist effective management and retrieval.

3.3 : Document version control

Consistent naming rules can link different versions of the same document, by including a version number as part of the title. This will also help to provide an audit trail for future tracking of document development; but does depend for success on disciplined use and careful tracking of versions. There is a danger of inconsistency if a document version is updated separately by different users without co-ordination, so that varying versions may exist each with different parts, but neither with all, of the full updated content. Well-developed and robust procedures are important for control of document versions in a multi-user environment.

The document name, and not the document extension, should be used to indicate the version number. Use of document extensions for version control will immensely complicate the mapping of document extensions to applications that can read them, creating a complex management overhead and the potential for conflict with later applications which may expect to use already allocated file extensions.

Example of version control information

Show document versions by structuring the title as:

<document name> - <version number>- <draft/fina l>.extension

as in:

Managing electronic documents - 0.4 - draft.doc

A common method for version control numbering is to use the ordinal number (1, 2, 3, etc) for major version changes and the decimal number for minor changes, as in:

ver: 0.5; ver. 1.0; ver. 2.7

A version 1.0 normally denotes a first document version given wider circulation – a document moving from personal to corporate workspace.

Footer information in documents is also useful for showing version information, and the location of equivalent paper documents.

3.4 : Folder titles

Naming principles can be applied to folders. Two ways in which this can be done are:

- using standard terms for themes and activities which recur across the organisation: for example, project organisation structures that are common despite differences in project focus
- using consistent logical labels to describe business activities and functions which are common across an organisation.

Standard folder titling can be applied at:

- the corporate level, applying organisation-wide rules

- the workgroup level, where more specialised rules reflecting local conditions may be appropriate
- the personal level, to assist the individual with organising and developing working documents.

Standard folder titling may be developed into a structure which aims to mirror appropriate parts of the established paper filing structure, where this is desirable. This approach is dealt with in section 6.2 and 6.3.

3.5 : Use of a thesaurus

A thesaurus is a structured list of preferred terms arranged in a logical relationships with each other, more formal than a simple list of keywords. Many new information management initiatives tend to make use of standard structured terminology. Where a department or agency has established use of a standard or specialist thesaurus, consider using these preferred terms in folder titles. It may be helpful to develop stronger links with other information and knowledge management initiatives, such as the Knowledge Network Research Online system (which is located at http://www.knowledgenetwork.gsi.gov.uk).

3.6 : Usability : length and readability

In the electronic environment, folder structures tend to contain more folders each containing fewer documents than occurs in the paper environment. This may lead to a greater depth in the folder structure itself. The length of folder (and document) titles can become an issue where a long pathway is built up through the folder hierarchy.

In most cases, an average of about 16 – 20 characters will be adequate, if care is taken to avoid repetition and redundancy. Long folder titles lead to very long pathways for an individual document, with the possible result that the relevant application is unable to open the document successfully.

Example of titling usability

An example of *poor* usability in a pathway name is:

Electronic Records \ Office Systems(EROS) \ Surveys of Government Departments \ 1999 – 3RMG 13.11 \ EROS Survey 1999 – Analysis and Results Process – 3RMG 13.11.2 \ Survey Forms Returned

better to use:

Electronic Records \ Survey 1999 \ Survey Forms Returned

and reference the file numbers elsewhere, if they are needed.

A balance must be struck between emulating the paper system, and recognising the different demands of usability and practical use which operate in the electronic environment.

4 : Standard settings : profiles, templates and formats

Summary : standard settings

- use the Document Properties box for metadata, but sparingly
- design standard templates for very common document types
- standardise storage and distribution formats
- avoid using dynamic dates and linked documents

This section deals with standard settings that can be used with document-creating applications, such as MS Word 97, to control variations in the documents which are generated. Standard settings can be built into templates, including the basic *Normal.dot* Word template, so that all documents based on that template use these settings. Standard settings should always be used with caution, since they can generate unexpected results, and may place unacceptable burdens on the end user.

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

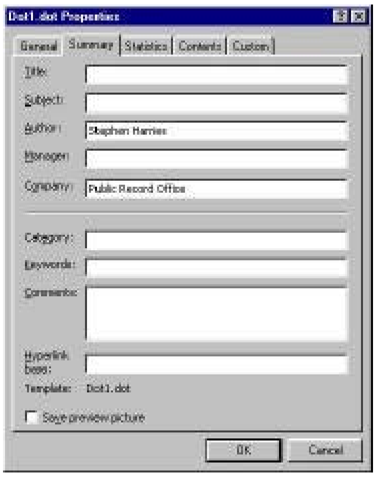
- keeping it *simple*: too much complexity will confuse and alienate the end user, and lead to potential misinformation
- keeping it *useful*: only those standard settings which have a demonstrable value should be used
- keeping it *flexible*: where it is hard to anticipate all valid variations, it is usually better to adopt a minimal approach that can be adapted case-by-case.

There are many potential metadata characteristics and template features that can be used in the MS Office application suite. Only a few of these can sensibly be put into practice in most government environments, unsupported by sophisticated EDRM systems. This section deals only with those which may be the most useful.

4.1 : Document properties

Most standard Windows applications contain some form of *Properties* area, which contains a set of fields that can be filled in as metadata, either by hand or automatically by the software application.

Example of Document Properties dialogue box in Word 97



Title:

Subject:

Author: Stephen Harries

Manager:

Company: Public Record Office

Category:

Keywords:

Comments:

Hyperlink base:

Template: Dot1.dot

☐ Save preview picture

In this example, the *Author* and *Organisation* fields are filled automatically from information accessible to the application; other fields can be filled in for individual documents at the time of creation or further editing. The Document Properties box can be set to appear automatically on first saving the document (and can also simply be dismissed by pressing the *Cancel* button).

Some advantages of using Properties are:

- standard key metadata terms accompany the document at all times
- support for document history tracking (although the level may be quite detailed)
- support for later migration to an EDRMS which is capable of capturing metadata from document properties information (many cannot do this).

Some disadvantages are:

- more work for the end user
- potentially misleading metadata where document production is shared: for example, where the *Author* field takes the last named editor, but the *Organisation* field remains the same
- in practice, no-one may bother to use the metadata gathered in this way effectively.

Though attractive at first sight, use of the Properties facility should always be well thought through and carefully justified – ask the question: *"why is this metadata necessary and what use will it be put to?"*

4.2 : Standard templates

Templates can be designed as basic standard forms for document types such as: letters, memos, requests, reports. They will:

- ensure a greater level of consistency in document (and record) production
- enable documents which should be kept as corporate records to be more readily identified
- support a closer integration of document production with line-of-business operations.

It is not feasible to attempt to design templates for every identified document type, or to construct variants for different folders. Only those document types which are in common use across the whole organisation should be candidates for a standard template.

Example of standard template settings

While the design of more specialised templates will depend on the nature of the document type and the business activity which it supports, there are some basic features which can be used for all types of document. Some of these features can be incorporated into the basic template for all documents generated by an application:

- headers can show a title taken from the Title field of the Properties
- header or footer can show organisational unit or workteam
- footers can show pathname, version number, and various forms of date.

4.3 : Dynamic updating - dates

In MS applications, it is possible to insert a generic date field which can be updated automatically by the application. These are convenient when used carefully, but will provide false information if used indiscriminately, particularly where different types of date are not clearly labelled and identified.

Example of dynamic dates

A *Date of Saving* field is updated each time the action takes place, and may be confused with other types of date. Use of these fields in a template should always be preceded by an appropriate phrase, as in:

Last edited on : {SAVEDATE}

so that its use for tracking edited versions is made clear, appearing in the document as:

Last edited on : 07/11/00

Use of a *{Today's Date}* field which is dynamically updated is not recommended

4.4 : Storage and distribution formats

Where 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 far as possible, so that current access and future migration problems are reduced.

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 MS Word 97 to save all documents in the current .doc 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.

  For example, use the Microsoft version of RTF, by saving all corporate documents in a .rtf format (which the application can be set to do automatically). These documents will be accessible by different application versions (e.g. MS Word 97 and MS Word 95) and by other word processors; but some formatting information may be lost in certain circumstances.

- Standardise on a **distribution format**, where documents are finalised and will not be changed in content.

  For example, a PDF rendition has the advantage of making documents effectively read-only, but requires the necessary Acrobat software to produce the rendition. This option is unlikely to be cost-effective for a large number of direct users, and will depend on some form of centralised or clustered storing function.

- 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 browser; but Office 97 products are unsophisticated at producing html renditions, the html syntax may contain proprietary elements, and it is harder to control document versions.

4.5 : Embed rather than link

Where it is desirable to include the contents of one document in another – for example, to include the contents of a spreadsheet in a text document - embed the content rather than using dynamic linking. While the latter approach will give a more up-to-date view of the information, it is extremely difficult to capture and manage changing versions of the document effectively over time.

If dynamic linking is unavoidable to provide up-to-date operational information, take a copy of the document at significant points of change and retain as a formal document version.

5 : E-mail and messaging

Summary : e-mail

- develop policies clarifying which e-mails should be kept
- develop procedures for managing messages within the e-mail system
- extend procedures to include use of shared drive folders when feasible
- develop guidance for managing e-mail composition and dialogues
- help individuals to manage their own mailbox

E-mail messages should always be treated as potential corporate records of the organisation. More and more departmental business is conducted by e-mail, replacing the conventional memo and, increasingly, the formal letter. Valuable material will be lost if e-mail is not managed in some way; but this can be difficult to do because:

- e-mail is not a simple record series, but a mechanism for transmission, so an e-mail system cannot be scheduled in its entirety
- retention depends on the content and context of the message, and is different for different messages sent or received by the same user, which must be treated separately
- essentially, e-mail is an individual channel, and is managed by the end user, or not at all.

There are three main approaches to managing e-mail records without the support of EDRM software:

- by a 'print-to-paper' policy – but this tends to work even less well than with word processed documents
- by managing within the e-mail system
- by saving messages to a shared drive.

Each approached is discussed below in more detail.

5.1 : E-mail usage policies

Develop clear policies to guide users on which types of e-mail message should be retained in the medium to longer term. These should cover:

- which messages a user sends that should be retained
- which messages a user receives that should be retained
- which dialogues should be recorded
- where drafts should be retained
- requirements for access to all these types of messages.

In addition, organisational policies should emphasise:

- an assumption that any e-mail message relating to departmental business may be kept as a record

- care in composing and expressing content
- expectations of privacy
- avoidance of inappropriate content.

5.2 : Managing within the e-mail system

The types of folders within an e-mail system follow the three-level workspace model described in the section summary for this section:

- **personal** folders are limited to individual access only, and cannot constitute a corporate record
- **shared** folders are a workteam space, where messages within an organisational unit can be stored and shared
- **public** folders are equivalent to corporate space.

The aim is to encourage users to store messages appropriately in one of these three areas. To be successful, the co-operation of the individual in regularly moving relevant messages from the personal mailbox to shared or public folders is required. Guidance should therefore always stress the benefits to the individual as well as the organisation.

Advantages of managing messages within the e-mail system are:

- all metadata relevant to the record is captured and preserved
- within a manageable environment
- with built-in filtering and deletion facilities available.

There are some **disadvantages**:

- e-mail messages are not integrated with other relevant documents or records in one structure
- so that parallel filing structures will develop, potentially including an individual's personal folder structure
- in addition, deletion does not ensure destruction, since the e-mail will be retained on back-ups.

Although probably not the ideal solution in the long term, this approach will provide valuable groundwork for the move to corporate level EDRM, by establishing good habits and practices in individual and team handling of e-mail as well as demonstrating the value of well-organised records.

5.3 : Saving to a shared drive

The option of saving messages to a shared drive has the advantage of bringing together all documents and messages relevant to a theme or activity in the same folder, and making this available for corporate access. It is, therefore, closer to the way in which e-mail messages would be managed in a full EDRMS. Unfortunately, the process of manually saving to a shared drive is rather cumbersome. This option would be best suited to a user population which has already developed good practices in handling e-mail.

User guidance will be needed on the appropriate *save* format and method to use:

- when to use the *Save as* … command and when to *Save attachments* separately. Where any significant information is contained in the body text of the e-mail itself, both the message and any attachments should be saved together in one operation.

Messages can be saved in various formats:

- a *.msg* format is convenient for use within the Outlook environment, but is proprietary and may be difficult to migrate over time
- a *.rtf* format is a (fairly) standard exchange format, which will embed any attachments within the message body, but will usually take a greater amount of disk space
- use of a*.html* format is not recommended here.

Message formats:

- transmission data, showing fields such as date of sending and receipt, recipients, subject title, should always be saved with the message text
- messages should not be saved to a shared corporate drive in any encrypted formats.

5.4 : Creating and replying to messages

User guidance on the composition of e-mail messages should cover:

- rules for addressing to main recipients and to c.c. recipients
- message length and use of attachments
- managing dialogues
- use of categories and labelling.

5.4.1 : Addressing messages

The basic rules for responsibility in filing an e-mail message are:

- the sender files a message sent within the organisation
- the recipient files a message sent from outside the organisation
- recipients marked as c.c. do not need to file the message.

Example of rules for addressing 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 on an Intranet or Public Folders instead.
- Consider whether e-mail is the appropriate channel to communicate this message.

5.4.2 : Message length and attachments

There are two broad approaches to the use of e-mail for formal business:

- using the e-mail purely as a wrapper for the substantive text, which is contained in an attached document, so that only the document need be saved
- composing longer text messages, which contain the text directly; the message itself is kept as a record.

The former approach requires management of the native document over time, and is unwieldy in many situations. The latter has the advantage that the message is plain-text based, and is easier for the user to produce.

The most appropriate form to use will vary according to the nature of the communication, but it is often better to encourage direct use of e-mail where appropriate, rather than extensive use of attachments – and this format is easier to maintain over time.

5.4.3 : Managing dialogues

E-mail messaging is an unstructured medium which will tend to become disorderly and tangled unless guided by disciplined procedures. Confused e-mail threads and much repetition of previous message text in dialogues will produce confused and repetitious records. Disjointed replies and the use of embedded messages are also sources of poor structure that are difficult to manage.

Examples of rules for managing dialogues

- Use clear and descriptive subject lines
- Indicate if no reply is needed
- Do not *re-send* 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 physical e-mail. It is better to create separate messages for separate topics, in the same way that a text document should have a single central focus.
- The organisation should consider making a business rule on the use of *reply with original text* feature. The two options are:

  to turn off the *reply with original text* feature, so that each sent message contains the text of the reply only; and should (if it is a significant message) be saved as a separate record

  to include previous text in replies, and identify a significant point at which the whole dialogue is saved as a record in one physical message – often, though, it can be hard to identify this point until some time has elapsed.
- Do not reply by annotating the original text at various points – it is better to group all reply text together in one place.
- Do not embed earlier e-mail messages within the current e-mail messages, since this makes the physical object difficult to file and manage.

5.4.4 : Use of categorisation and optional flags

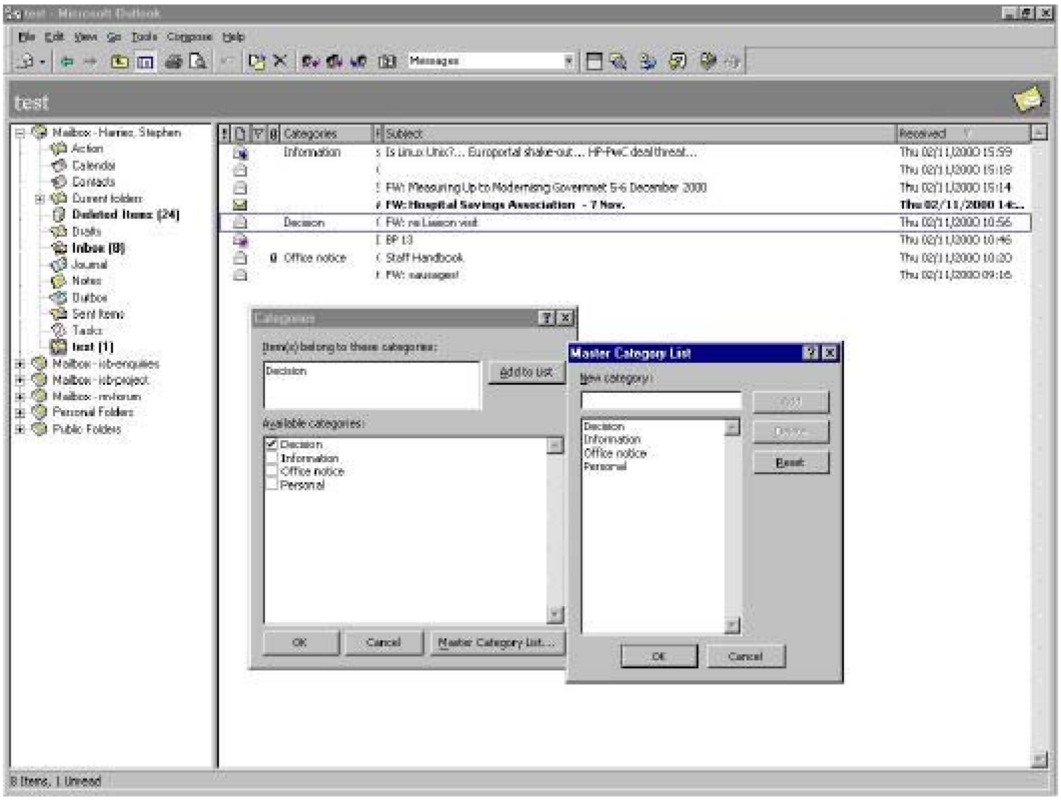
MS Outlook contains a Master Category list of category terms, which can be attached as labels to an individual e-mail message. The standard terms can be adapted by adding and removing terms from the list. These terms can be used to identify categories of messages which should be handled in particular ways.

Categorisation can be used to:

- help the individual manage and respond to their e-mail at a personal level
- help to identify important messages that should be filed, from ephemeral messages that should not.

Example of use of categories

A list of terms such as: For Decision, For Information, Directive, Personal can be easily constructed. Terms added to a message by the sender will be displayed in the recipient's mailbox (as long as the appropriate *current view* is set up).



Categories	Subject	Received
Information	Is Linux Unix?... Europortal shake-out... HP-PwC deal threat...	Thu 02/11/2000 15:59
		Thu 02/11/2000 15:18
	FW: Measuring Up to Modernising Government 5-6 December 2000	Thu 02/11/2000 15:14
	FW: Hospital Savings Association - 7 Nov.	**Thu 02/11/2000 14:...**
Decision	FW: re Liaison visit	Thu 02/11/2000 10:56
	BP 13	Thu 02/11/2000 10:46
Office notice	Staff Handbook	Thu 02/11/2000 10:20
	FW: sausages!	Thu 02/11/2000 09:16

Categories

Item(s) belong to these categories: Decision

Available categories:

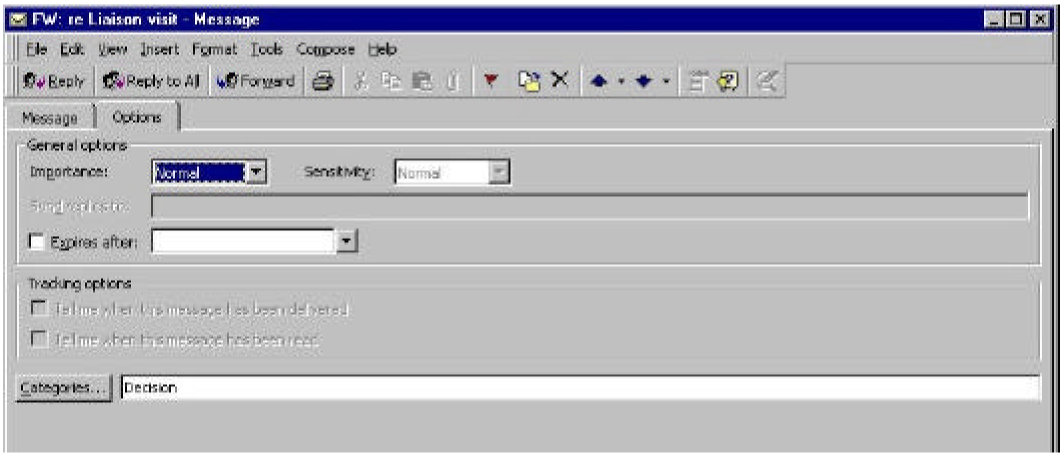
☑ Decision
□ Information
□ Office notice
□ Personal

Master Category List

New category:

Decision
Information
Office notice
Personal

Other message options that can be set to help distinguish important and unimportant material are: *Sensitivity level* – Normal, Private, and Confidential; and *Expiry date* – after which display of the message will be struck through.


FW: re Liaison visit - Message
File Edit View Insert Format Tools Compose Help
Reply
Reply to All
Forward
Message
Options

General options

Importance: Normal

Sensitivity: Normal

Send replies to:

☐ Expires after:

Tracking options

☐ Tell me when this message has been delivered

☐ Tell me when this message has been read

Categories... Decision

5.5 : Managing the InBox

User guidance on managing a personal mailbox should cover:

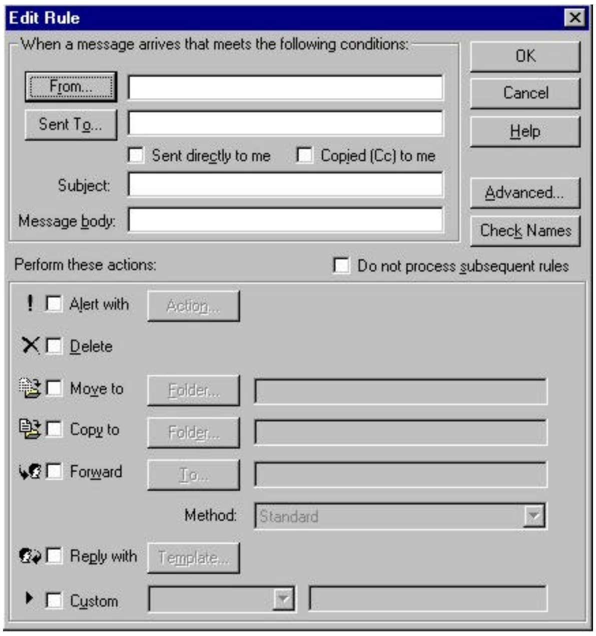
- the value-added benefits of structuring any *personal folders* within the individual mailbox to be consistent with folder structures used to store documents in both personal and corporate workspace drives

  This will help to integrate different filing structures at the logical level, and is a useful step towards integration at the physical level; as well as introducing personal information management disciplines.

- the need to delete messages and working copies, where these have been saved into a corporate filespace and are no longer of local interest.

  This will help to ensure that in the longer term, duplicate copies of information items are destroyed – important for managing freedom of information – and to reduce the likelihood of alternate versions arising.

- the potential for automatically routing incoming and outgoing mail to nominated folders, using the InBox Assistant, where standard types of message can be pre-determined according to characteristics recognisable to MS Outlook.



When a message arrives that meets the following conditions:

From...

Sent To...

☐ Sent directly to me ☐ Copied (Cc) to me

Subject:

Message body:

Perform these actions: ☐ Do not process subsequent rules

! ☐ Alert with Action...

✕ ☐ Delete

☐ Move to Folder...

☐ Copy to Folder...

☐ Forward To...

Method: Standard

☐ Reply with Template...

☐ Custom

This can help to build structured sets of records, but should only be used with material that can reliably be identified by metadata characteristics.

- caveats on using the auto-archiving facility, which automatically archives (i.e. removes from the InBox) messages after a set period – to be used with care!

6 : Use of shared network drives

Summary : shared drives

- encourage ‘publish and point’ rather than multiple duplication
- develop logical and useful filing structures for shared drives
- develop common terminology and links to the paper filing systems
- establish control over folder creation
- consider use of electronic zero files
- develop ‘good housekeeping’ for synchronising and deleting documents

This section deals with the use of shared drives for managing corporate documents. In most local area network architectures, network drives appear to the user as various logical drives, typically arranged as:

- a corporate-wide shared drive, containing documents relevant to the whole organisation
- a branch, or divisional shared drive, containing documents relevant to a single organisational unit
- a personal drive (for example, a P: or U: drive), containing documents relevant only to the individual.

In all cases, it will be necessary to identify clear and acceptable use policies for all three categories of drive. Good practices in managing electronic documents should be initiated in both the user workspace and the corporate space – good practice starts with the individual.

6.1 Publish and point

A *publish and point* policy is a method of controlling the duplication of a document which is being widely circulated. Instead of attaching the document to an e-mail message, which gives each recipient an individual copy, a read-only version of the document is placed on a shared drive – *published* – and a *pointer* or shortcut is e-mailed to alert intended recipients. Recipients can then retrieve the document from the shared drive as required.

This policy will:

- help to encourage a culture of sharing documents, within a forum and as an organisational resource, rather than as individually owned items
- encourage users to think more carefully about the most appropriate method for publishing information to recipients and to treat these consistently as formal corporate documents
- reduce keeping of multiple working copies in the folders of many individuals.

A *publish and point* policy will tend to decrease the requirements for individual document storage, but increase the need for network bandwidth by generating more traffic from common storage.

6.2 : Filing structures

Where there is a significant number of electronic documents stored on a shared network drive, a basic general filing structure should be established. Where a division or branch (and any project–based structures) has specific filing structures, these should aim to conform to the principles of a general filing structure to prevent divergent practices and application.

Basic filing structure on shared drives should

- use simple but logical structures which meet the needs of both the organisation and the users
- *not* use individual names or position titles for directory or folder names
- use names which identify logical elements, such as business functions and activities or theme: sub-theme relationships
- have an established responsibility for creating and naming folders.

While the need for good filing structures in a shared network drive is primary, end users should also be encouraged to use consistent filing structures in their own group and personal workspaces. This will help with the co-ordination between working papers and formal finalised documents, and will ease retrieval and access across all workspaces for the individual.

Common terminology

Use of a common terminology is essential to integration; planning the use of shared drives should be done in conjunction with thinking about naming conventions, as described in section 3.

- work towards consistent use of common terminology across all departments and units of the whole organisation
- develop formal liaison mechanisms between those responsible for records at the local level to establish and enforce these conventions
- where feasible, make terminology in the shared network folder structure consistent with terminology in the paper filing system
- make links with entries in the inventory of record collections.

6.3 : Relating to paper filing system

The organisation of a shared network drive can usually be made to reflect the paper filing structure so that electronic documents are stored in a manner compatible with their paper counterparts. This may be achievable by building a hierarchical ‘folder within folder’ structure using Windows, to simulate the structure of a paper fileplan.

Some considerations are:

- there is little point in building a paper-based structure in electronic folder form which is not working well in the paper environment; and in most cases, a formal move towards implementation of EDRM will probably require some re-thinking of the approach and structure which is most appropriate for the new environment

- electronic structures tend to be broader and flatter – have less depth – than their paper counterparts; it is important to control the number of levels to retain usability; carefully consider the categories and terminology used at higher levels – in general, more than about 4/5 levels to a hierarchy can quickly become confusing and cumbersome
- alphabetical folder titles are generally more usable (in the electronic environment) than numerical fileplan / classification reference numbers and using both together will produce very long folder titles
- paper filing systems tend to use longer names than are comfortable in a Windows environment, resulting in file directory displays where the relevant, lowest part of the hierarchy is off-screen and not visible; in these circumstances it is also possible, when the full pathway of a document is constructed, to exceed the limit with which a software application can deal and thereby render the document apparently unusable.

6.4 : Control over folder creation

Where the folder structure on shared drives is formalised in this way, clearly set out rights and responsibilities for folder creation and, where this is restricted, allocate these to specific roles. Consider:

- the extent to which a formal link to paper filing control systems, and the information which they contain (such as retention and disposal information) is desirable
- the role of local records officers in maintaining electronic filing structures
- the extent to which workgroups are able to create electronic folders themselves
- mechanisms for guiding and controlling the use of terminology.

Use of Zero files

A Zero file is a file which contains metadata about a series of folders, recording common information about that series, including its history, retention and disposal, opening and closing dates, and relationships to other record series. A zero file is sometimes used in paper filing systems, and can be adapted to the electronic environment. Potential uses include:

- as a link to the entry in the inventory of record collections for a set of electronic folders
- as an updateable link to parallel paper series structures, to maintain integrated control, whether the electronic or paper version is considered to be the formal record copy
- recording any access restrictions
- identifying users who are responsible owners
- retention beyond the life of the electronic folders, to document actions taken on the material (important for Freedom of Information)

6.5 : Balancing drive usage

Gradual extending records management disciplines to the shared network drive environment will eventually involve decisions on technological support platforms and network bandwidth; complementary technical policies and procedures will need to be developed. Consideration should be given to:

- the risks of lost documents in a shared network environment, where more reliability is expected
- the need to provide back-up and (perhaps) mirrored storage
- the implications of shared storage for network traffic and bandwidth requirements
- clear identification of material that should be entrusted to a shared drive and material that should be entrusted to the non-shared environment (and therefore printed to paper).

The move to full EDRM will require decisions on these kinds of issues in any case.

6.6 : Disposing of documents

In all cases, 'good housekeeping' of both shared and personal drives is essential to maintaining long-term viability, removing material which should no longer be kept, whether classed as document or record. Since good management in this semi-structured environment depends largely on the application of developed procedures and is not supported by corporate-wide document management software systems, some duplication and redundancy will probably be necessary to ensure good access for business purposes. Guidance should aim to reduce this to the right balance for the organisation – excess redundancy also works against usable access.

Guidance is needed for removing:

- unnecessary duplicates of final documents
- working copies which are no longer required
- documents which have no continuing value.

Users of local drives and personal areas of a network drive should also be encouraged to perform basic housekeeping. Regular use of the Windows Explorer *Find* facility for documents created and modified in a given period of time, will help ensure that locally held files are deleted or copied to the relevant shared drive as appropriate. Local drives should not be used for long-term storage of corporate level documents.

Laptops and synchronisation

Laptop and handheld computers are now widely used, at all levels of an organisation. These can cause particular difficulties when used in conjunction with a standard desktop PC, where documents are duplicated for working on in a different location. Lack of proper procedures may result in documents existing in different and potentially conflicting versions; it is particularly important to

- maintain a working structure on a laptop which is consistent with that visible from the main desktop machine
- develop a disciplined approach to updating document versions

- nominate a single storage location for documents in development, to hold the primary version and later updates.

File synchronisation facilities such as Windows Briefcase, which keep track of changes to particular files, can help to manage this duplication, as long as use of the facility is clearly understood. Windows is not designed as a robust medium for handling file conflicts, and will not substitute for sound agreed working procedures, particularly where several members of a workteam are working on the same documents.

A similar synchronisation facility is often used with MS Outlook and MS Exchange to synchronise folders in a local copy of an e-mail mailbox held on a laptop, with the same recipient's primary network mailbox. Many people use this facility to create and reply to e-mails using the local laptop copy, that are later uploaded to the main mailbox for despatch. The synchronisation facility harmonises changes in both main and local mailbox versions. Potential difficulties can arise where two separate copies – local and main copy – of a message have been separately edited producing conflicting versions. Careful following of a procedure to ensure that all local changes have been uploaded to the main mailbox before editing existing main mailbox versions will minimise potential replication conflicts.

6.7 : Secure shared drive

A secure record drive is a shared network drive which has been configured in such a way as to prevent the amendment or unauthorised deletion of documents which have been saved to the secure drive. With such a mechanism, organisations *may* feel able to treat the electronic documents stored in this way as the formal corporate record, even though a paper copy may also exist. Where this is the case, they should be stored within a separate structure from electronic documents which are not treated as corporate records; with clear definition of who has the right to add to, or delete from, the drive.

- Use a separate logical hard drive with *read-only* settings to prevent any changes being made to documents which have been saved to the drive.
- Users should be able to *read* and *create* documents, but not be given edit rights to existing documents.
- Ensure appropriate back-up and recovery procedures, and maintain the necessary level of access security at the operating system level.
- Assess the criteria and risks involved in this approach and clearly identify the types of document which it may be acceptable to manage in this way; a secure drive does not provide the same level of assurance as a fully managed EDRMS.

Departments and agencies should be aware that, although this method can provide reasonable sound storage of documents in the short term, there may be problems with migrating the material to a full EDRMS in due course. The Windows directory structure does not easily provide document and folder level metadata that will support a structured migration to an EDRM system; and although migration can be achieved it may be a relatively expensive process.

6.7.1 : Sensitive information

The shared drive areas where corporate documents are made available should be capable of control by read/write permissions and by password control. Password control will enable control of user access to certain documents, either by:

- saving the document with password control if the application software supports this (as for example MS Word does) and copying the documents to the drive in this form
- placing password control on the entire logical drive.

This may provide some basic access control, but the method has limitations:

- application software password control is not particularly sophisticated
- circulating a password to a number of different people is inherently insecure
- in a read-only drive, the document cannot be easily changed to amend or remove the password, because it is tightly bound with the contents.

In practice, documents containing any sensitive or classified information should probably not normally be storage on a secure shared drive.

7 : Agenda for action : identifying steps to practical implementation

Action step	Who should be involved?	Does a policy exist? Is it explicit? Is it followed?	Build on existing practice? Adapt existing practice? Borrow from elsewhere?	Initial ‘To do’ List
Naming conventions				
Establish standard name forms and terms				
Develop rules for structuring titles				
Establish document versioning				
Consider use of a thesaurus				
Standard settings and templates				
Identify uses of Document Properties				

Action step	**Who should be involved?**	**Does a policy exist?** **Is it explicit?** **Is it followed?**	**Build on existing practice?** **Adapt existing practice?** **Borrow from elsewhere?**	**Initial ‘To do’ List**
Identify potential standard templates				
Standardise on distribution formats				
Standardise on storage formats				
E-mail management				
Develop rules governing keeping of e-mail				
Develop structures for public/shared folders				

Action step	**Who should be involved?**	**Does a policy exist?** **Is it explicit?** **Is it followed?**	**Build on existing practice?** **Adapt existing practice?** **Borrow from elsewhere?**	**Initial 'To do' List**
Develop guidance for composing messages				
Consider possible uses of shared drive storage				
Shared network drives				
Promote a 'publish and point' policy				
Build links to paper filing				
Consider use of zero files				
Develop mechanisms for document				deletion

Section 3 : How to start putting these steps into practice?

Summary : practical steps

- identify and consult all relevant stakeholders
- consider the impact on business and IT management
- prioritise key areas where results can be achieved
- develop local experience and commitment

This section deals with:

- consulting the range of stakeholders
- prioritising and planning
- developing local expertise.

8 : Stakeholders

Although the topics covered here are of primary interest to records and information managers, there are a range of stakeholders who will have an interest in the areas covered in this toolkit:

- several aspects involve the use of technical resources – in particular drawing on network resource – which are resource elements within the corporate IT infrastructure
- the implications for creating, organising and using information may have an impact on working practices and the way business processes are carried out
- end users will need to be engaged from a personal perspective because success depends on compliant behaviour which cannot be policed.

All these groups will need to be consulted in developing practical working procedures, and may need to be drawn directly into the process of development at the appropriate point.

8.1 : Corporate IT infrastructure

Corporate and local IT staff and network administrators will need to be involved with decisions which have implications for:

- network infrastructure and network bandwidth
- provision of drives, servers and back-up mechanisms
- configuration of back office software
- configuration of operating systems
- configuration and provision of desktop applications.

8.2 : Business managers

Business managers will be concerned about the implications for:

- the application of business rules
- the development of procedures and the effect on the business processes
- the implications for operational practice
- the information needs of operational staff.

8.4 : End Users

End users are primarily concerned with the earlier parts of the document lifecycle: creation and operational use. This is the main group which needs to be convinced of the value in following good practices as outlined in this toolkit, by demonstrating:

- the value of managing documents at the personal level, making information easier to find and reducing information overload
- the responsibilities in creating and capturing organisational information
- the advantages of establishing a custodian for certain types of document – e.g. project documentation
- the advantages of maintaining co-ordinated or integrated filing structures, for example, between e-mail folders, personal drive folders and shared network folders.

9 : Prioritisation : planning a way forward

Except in the very smallest organisations, it is unlikely that the measures described here can be put into place across the whole organisation in one process. Initially, significant effort will need to be put into:

- establishing over-arching corporate level policies and standards (which should be transferable to the full EDRM environment)
- building local commitment and agreement from users to putting these measures into practice
- developing local expertise through training and organisation.

A strategy for building commitment across the organisation is to identify key priority areas that will provide high profile examples to encourage others to follow, and that offer a platform for developing transferable policies and procedures. Such a phased approach will enable proper consideration to be given to local conditions within a corporate context.

9.1 : Identifying key target areas

In identifying key target areas, consider:

- the need to tackle key business processes and transactions which are important for accountability, for example: the interactions between policy advisors; primary line-of-business processes
- the feasibility of establishing good practices in these areas, including the internal political issues
- the relative enthusiasm of end users in putting measures into practice
- the type of documents which are generated, and the technological environment in current use
- the ability to generate 'quick wins' with most effective use of effort.

At the level of the whole organisation, consistent corporate level standards should be developed as a framework for local implementation, including:

- guidance on what types of document should be kept in a formal manner as corporate information and records
- agreement on quality standards
- clear co-ordination with the existing 'print to paper' policy to guard against loss of paper records where these are still required, whilst taking forward the electronic agenda
- consistent strategies on the larger questions, such as a risk analysis of the use of shared network drive filing structures for the storage of authentic corporate documents.

9.2 : Local and central records control

In extending central principles to local branches, there needs to be a clear understanding on the implications of adopting wider corporate policies and standards, and of the relative roles and responsibilities. Local agreement will need to be established branch by branch; within this process, there may be scope for incorporating more specialised branch and workgroup standards.

Once the scope and purpose is understood and agreed with staff, such local agreements should be formalised and published locally, on an Intranet or similar mechanism. An document which explains the local benefits on offer by agreeing to follow the practices outlined, and the responsibilities inherent in doing so, is one mechanism that can be used – sometimes this is called an *Offer document* because it shows what is on offer.

9.2.1 : Local document/records officers

Where possible, establish local document/records advisor or business records officers, who have responsibility for setting up and maintaining local filing structures and acting as local centres of expertise. This role requires:

- a sound understanding of business objectives, corporate records policies and procedures
- knowledge of the office systems and software in general use
- responsibility for ensuring security and access
- the ability to create and maintain directories in a shared network space, and to maintain and review working procedures and naming conventions
- the ability to promote good practice to users.

It will be essential to ensure that these local officers build and retain strong links with corporate records management structures and with broader information management strategies.

9.2.2 : Workgroup mentors

Workgroup mentors are end users who have acknowledged best practice skills and can act as initial points of advice for their colleagues, and as localised channels for promoting cultural change in the end user population as a whole. A good strategy for establishing best practice in managing documents will encourage peer mentoring, where mentors can act as ambassadors for good practice.