

Information Management infoKits



www.jiscinfonet.ac.uk

- Information Management infoKit** 6
 - What Is Information Lifecycle Management?..... 7
 - Taking A Holistic Approach To The Management Of Information 7
 - The Advantages Of Taking A Holistic Approach..... 7
 - The Information Lifecycle Model 8
 - Variations To The Lifecycle Model..... 8
 - Rationale for model selected 8
 - From theory to practice 9
- Creation 10
 - Creating The Right Information..... 10
 - Creating Reliable Information 11
 - Data Quality..... 11
 - Data Currency 11
 - Status And Version Control..... 11
 - The Right People Creating Information 12
 - Proof Of Provenance..... 12
 - The Dangers Of Over-Restricting Access..... 12
 - The Benefits Of Unfettered Access..... 12
 - Creating Information In Appropriate Formats 13
 - Capturing The Right Metadata..... 14
 - Metadata Types..... 14
- Active Use..... 14
 - Define The Purposes For Which Your Information Can Be Used 15
 - Locating And Accessing Information..... 16
 - Who Needs Access To The Information? 16
 - Restricting Access..... 17
- Semi-Active Use 17
 - What Information Is Held And Why?..... 18
 - Defining The Journey From Active, To Semi-Active Use..... 18
 - Retaining The Context..... 19
 - Continued Maintenance 19
 - How Long Should Information Be Kept For? 19
 - The Drivers Governing Information Retention..... 19
 - Risk Management 20
 - Assessing The Value of Information To the Organisation 20

Defining Value	20
Appropriate And Cost-Effective Means Of Storing Information	21
Storage Options	21
Out Of Sight Shouldn't Mean Out Of Mind	21
Is Your Information Safe?	21
The Overlooked Importance Of 'Good Housekeeping'	22
External Service Providers	22
Final Outcome	22
Ensuring Continued Access To Information	23
Controlling The Disposal Of Information.....	24
When Has Deleted Information Really Gone?	24
An Auditable Process	24

EMAIL MANAGEMENT

Email Management	25
The rise and rise of email.....	26
The Risks Associated With Email	26
Creation	27
Ensuring Appropriate Email Use	28
Appropriate Use Policy	28
Making Staff Aware	29
Enforcement	29
Encourage Staff To Create Fewer Emails	29
Providing And Promoting Alternatives.....	29
Promoting Good Practice	30
Improving Your Email.....	30
Titles & Other Metadata	30
Content	30
Email Disclaimers.....	31
The Case 'For' Disclaimers	31
The Case 'Against' Disclaimers.....	31
Active Use.....	31
Monitoring Email Use	32
Remote/Home Use Of Email.....	32
Outsourcing Your Email Provision	33

Email Security	34
Passwords & User Behaviour.....	35
Account Maintenance	35
Making Best Use Of Your Email Software	35
Semi-Active Use	36
Identifying Emails As Records	37
Next Steps	37
Managing Emails As Records.....	38
Authenticity	38
Completeness	38
Reliability	38
Fixity	38
Managing Email Retention	38
By What Criteria Should Email Retention Be Decided?	39
Retention Based On Content	39
Separating The Wheat From The Chaff	39
Managing Email Retention In Context	39
What Happens When A Member Of Staff Leaves?	40
Finding Emails.....	40
The Advantage Of Central Storage	40
User Behaviour During A Legal Discovery Exercise	41
Final Outcome	41
Archiving & Preserving Emails.....	41
Deleting Emails	42
Has Your Deleted Email Really Gone?	42

RECORDS MANAGEMENT

Records Management	44
What Is Records Management?	45
Why Is Records Management Necessary?	46
Creation	46
What Is A Record?	47
Creating Authentic Records	48
Why Is This Important?	48
How To Create Authentic Records.....	48
Creating Complete Records.....	48

Why Is This Important?	49
How To Create Complete Records	49
Creating Reliable Records	49
Why Is This Important?	50
How To Create Reliable Records	50
Fixity & Declaring Records.....	50
Why Is This Important?	50
How To Declare Records	51
Active Use.....	51
Managing Version Control	52
Why Is This Important?	52
How To Maintain Version Control.....	52
Retaining The Audit Trail	52
Why Is This Important?	53
How To Retain The Audit Trail.....	53
Managing The Master Copy.....	53
Why Is This Important?	54
How To Manage The Master Copy	54
Protecting Vital Records	54
Why Is This Important?	54
How To Protect Vital Records	54
Semi-Active Use	55
Undertaking A Record Survey	56
Why Is This Important?	56
How To Undertake An Information Audit.....	56
Click for the Record Survey Guide	56
Retention Management.....	56
Why Is This Important?	56
How To Manage Retention.....	57
Final Outcome	57
Record Appraisal & Disposal	57
Why is this important?	58
How to appraise & destroy records	58
Permanent Preservation & Curation	58
Why is this important?	58
How to preserve records	59
Disclaimer	60

MANAGING THE INFORMATION LIFECYCLE

INFOKIT



www.jscinfonet.ac.uk/infokits/information-lifecycle

What Is Information Lifecycle Management?

The information that your institution creates and uses can either represent an asset or a liability. Into which of these camps it falls is largely dependent on how it is managed. Put simply, the concept of information lifecycle management is about making sure you ask yourself the right questions at the right time regarding the management requirements of internally produced information. It does this by breaking down the 'lifecycle' that all information moves through into four distinct phases and identifying what are the most pertinent issues that influence how information should be managed during each phase.

Consideration of these issues at the outset helps ensure the effective management of your internal information throughout its entire lifecycle: from cradle to grave.

Taking A Holistic Approach To The Management Of Information

Unfortunately there is not a 'one size fits all' specification for what is required to ensure good information management. A host of factors, both from within the institution (operational) and from outside it (regulatory, legal) will need to be considered. Moreover, these influences will vary over time and are dependent upon the type of information being created, its purpose, content and usage. What is therefore required is a consistent framework within which the management of information can be considered. This framework needs to be flexible enough to accommodate the variety and range of information now being created and ultimately to ensure that the right decisions regarding its management are being considered and made at the right time throughout its 'lifecycle'. This kit outlines the basic lifecycle framework, underpinning the related Records Management and Email Management strands in providing a practical approach to Information Management.

The Advantages Of Taking A Holistic Approach

Following the approach outlined within this infoKit will help ensure that the management of information created within your institution is consistent, proportionate and fit for purpose.

It is not dependent on the installation of expensive new technology nor does it assume that all information will be captured and managed in a single place by a single system. Instead it seeks to provide a conceptual framework which can be applied whenever and wherever a new system or process is to be introduced, or as part of a review of the management of information created by existing systems and processes.

The following table illustrates some of the key advantages of managing information via the lifecycle method and how they are realised.

Advantage	How?
Consistency	By following a common model and addressing the same fundamental questions, this approach ensures a consistency in the way in which information is managed regardless of the particular system it is created by.
Inclusiveness	This approach is equally as useful when considering the management of ephemeral information and raw data as it is formal business records. It also applies regardless of the format of the information, be it electronic or hard copy.

Pro-activeness	Following the model requires you to look to the future and what the management implications for a particular type of information are likely to be in the months and years ahead, as well as those you face now. This helps you to forward plan and avoid unpleasant surprises.
Proportionality	It is up to the user to decide which elements of the lifecycle model are relevant to the information concerned and to their individual circumstances. It does not seek to impose a heavy management burden (and cost) where such measures are not warranted and where a more lightweight approach is called for.
Flexibility	Because of the generic nature of the model it is not dependent upon any particular technology. Its approach is likely to be equally valid as and when new technologies emerge, thus further demonstrating the advantage of consistency. The way in which the model's recommendations need to be enacted will inevitably vary from system to system and process to process, but the underlying principles on which they are founded will remain constant.

The Information Lifecycle Model

The model of the information lifecycle used as the basis for this infoKit is a simple one based on four main phases:

1. Creation
2. Active Use
3. Semi-Active Use
4. Final Outcome

Variations To The Lifecycle Model

It should be noted that this is not the only version of the information lifecycle in existence, nor does it in any way represent the definitive version. A quick search of the web will locate several examples of lifecycle models, some very similar to those outlined previously, others substantially different.

Alongside those using the lifecycle methodology as a framework for managing internal information are others who are adopting the same fundamental 'cradle to grave' approach to the management of [library materials](#) or [storage management](#). This helps demonstrate the wide applicability of the underlying concept.

Of those using the lifecycle model for information management, some have more complex models which include a [greater number of phases](#) whilst others [use fewer](#).

Indeed there are those who believe the concept of the lifecycle to be fundamentally flawed with regards to information management and argue instead that the notion of the records continuum represents a more useful and practical model, particularly when managing electronic information. This view largely originates from and is particularly [prevalent in Australia](#).

Rationale for model selected

The one thing which unites all of the different variations and approaches outlined above is their concentration on taking a holistic, 'cradle to grave' perspective. With this consistent core principle established, exactly how the lifecycle is defined can and should vary according to the purpose for which it is being applied. None should be considered wrong, so long as they are comprehensive and fit for purpose.

With this in mind we believe the version of the model we have adopted for this infoKit is the best fit for our purposes due to its following characteristics:

- a clear chronological structure

*"All records have a life cycle from creation/receipt (birth), through into the period of active currency (youth), thence into semi-currency, e.g. middle-aged closed files that are still referred to occasionally, and finally either confidential disposal or archival preservation. In the digital age it is especially important to introduce conscious management at the earliest possible stage as this will determine the ultimate extent of control over electronic material"*¹

- clearly defined phases which users can relate to
- a consistent focus which does not combine different concepts such as management operations (e.g. 'evaluation' or 'applying retention schedules') and chronological phases within the same model, and
- breadth of application through avoidance of narrowly defined professional jargon.

From theory to practice

The following sections map the four phases of the information lifecycle and raise the generic questions which it is suggested you should think about with regards to the information that is being, or will be, created. Of course the term 'information' covers a huge variety of formats, media, technology and content and it is likely that the generic questions outlined within the lifecycle model will need to be further refined to address differing needs.

That is why this infoKit also includes applied sections where the concept and framework of the information lifecycle has been used to provide additional and specific guidance on the management of particular types of information. At present this includes guidance on the [management of records](#) and [emails](#) but it is envisaged that this list will grow in the future as more candidates for inclusion are identified.

The objective of these sections is to provide guidance on the management of these particular types of information that has been further refined to make it as detailed and specific as possible. This guidance will always follow the same lifecycle model and will build upon the generic questions and issues raised within it, but will add further detail where the specific requirements of that type of information warrant it.

This approach ensures the consistency of management referred to earlier, avoids the duplication of material (as some guidance will always be the same regardless of whether we are talking about formal records, emails or databases) and ensures that the specific topics are covered in as comprehensive and relevant a manner as possible.

¹ University of Edinburgh - Records Management Policy Framework
http://www.recordsmanagement.ed.ac.uk/InfoStaff/RMstaff/RM_framework.htm

Hopefully these applied sections will make it even easier for you to apply the lifecycle model to your own individual situations and thus help make the leap from theoretical model to practical application.

Creation

Creating information is often the easy part and appears at first glance to require little thought or planning. After all the whole drive of the IT industry in recent years has been to empower the user to create and manipulate information as quickly and easily as possible. Quantity, however, does not necessarily equal quality. Indeed it can often help contribute against it. Sometimes this may not matter. A hastily scribbled 'to do' list serves its purpose so long as it reminds you of what you must do and when you must do it by - assuming of course that you can find it when you need it. It is of little consequence whether it is typed into a word document, listed in an online diary or scribbled on the back of the proverbial envelope. Nor does it much matter whether it contains spelling mistakes or abbreviations only known to you. A completely different set of rules and acceptable quality standards apply when drafting of your annual report, designing a system for handling contracts or entering data within your personnel database.

The questions to be addressed during this phase are largely aimed at ensuring that the information created is fit for purpose and that it is actually capturing appropriate and reliable content. They include the following questions:

- Are you creating the right information?
- Are you creating reliable information?
- Are the right people creating it?
- Are you creating it in the most appropriate format?
- Are you capturing the right metadata?

Creating The Right Information

Information may be created for many different purposes. It may be deliberately created solely to inform others through its content. Alternatively it may be that its creation is merely the by-product of a process where its true value lies mainly in providing evidence that the process in question has occurred (for example a receipt for goods purchased). Either way it is important that the information in question is fit for purpose.

An example of a typical set of information which generally serves its purpose well is that which is created as part of the administration of a business meeting:

- The agenda: provides required factual information such as details of where and when the meeting is to be held, what is to be discussed and in what order so that everyone comes to the meeting equally and fully prepared
- Background papers: provides attendees with the information they will require to make informed decisions during the meeting
- Minutes: provides an agreed evidential record of what took place during the meeting

When designing a new process or system, it is worth considering what information you should be creating and why. For example, when documenting a new process, is it sufficient just to know that a stage in the process was completed or is it important to also know who completed it and when? This will depend on the nature of the process being undertaken, its importance and formality and a host of other factors. The important thing is that these issues are considered.

It is also important to ensure a consistency of approach to information creation across operations. It is less than ideal if a project being managed in one department creates a comprehensive set of documentation, whereas a similar project in another department creates next to nothing. Defining an agreed document 'set' to be used in such circumstances can be beneficial in terms of ensuring the right information is being created across all projects. The [JISC infoNet Project Management infoKit](#) includes an example of such a document set for project management and how it is used to ensure that each stage of a project is documented appropriately. Adopting this approach also has the benefit of making it much easier to compare information between projects.

It should be remembered that it is also possible to create too much information. This might not seem an important issue in an age where it is so easy and cheap to transmit and store information but it can easily lead to hidden costs and considerable user frustration. For example, it might be very useful for the administrator of a database or content management system to know when a change has been made to its content, but a system which generates an automatic email informing all users of every edit made will result in thousands of unnecessary emails being sent and considerable frustration on the part of staff who repeatedly receive worthless messages.

Creating Reliable Information

It is important that people are able to trust the information they are using. Often they will be relying on it as the single source of truth against which decisions will be made. It is not difficult to imagine the risks to the interests of individuals and the organisation as a whole if the figures in a budget spreadsheet are wrong, an employee's home address on the staff database incorrect, or the plans given to a builder out-of-date.

Human error is not always to blame when unreliable information is created. Simple things such as the wrong date and time settings being applied within a system can instantly lead to inaccurate information being created with documents or database entries seemingly being created on the 1st January 1900. Likewise it is common to find all documents apparently being created by a single person, simply because they were responsible for creating the original template, or happened to install the software on the network.

Data Quality

Where human error is to blame there are often ways in which the risk of it occurring could be reduced. Designing a system where the administrator is expected to type in each member of staff's name as a free text field is almost certain to lead to spelling mistakes, duplicate entries and other inconsistencies. These would largely be eliminated if the administrator was forced to select each name from a pre-defined pick-list. The margin for error is reduced still further if that pick-list could be provided direct from the main personnel database.

Data Currency

Users need to know that the information they are relying on is as current and up-to-date as possible. There is nothing more off-putting to a user than finding that the information they are relying on was last updated two years ago and has been superseded many times since. Who is to be responsible for updating content, how frequently this must be performed and what the 'triggers' to doing it will all need defining.

As ever, fitness for purpose is what counts. For example, many institutions will perform a proactive annual check of the personal information they hold on their staff to ensure it is all current (whilst also reacting to any changes they are informed about throughout the year).

Status And Version Control

However frequently your information is updated it is important that users can be confident that they are looking at the most recent version. Also that they know whether or not it is still information in draft and liable to further change, or whether it has been finalised.

Some examples of simple but effective measures for ensuring that version control is ensured can be found in our [Managing Information to Make Life Easier: A Guide for Administrators](#)

The Right People Creating Information

It's probably a safe bet that you wouldn't want the college nurse to be responsible for drafting your commercial contracts, nor for your procurement officer to be writing advice for students on meningitis. It is important that those responsible for creating information possess the authority and the ability to do so. This may require careful consideration of which functions and/or individuals within the organisation are trusted to create the information in question.

Proof Of Provenance

Once such responsibilities have been defined, it is usually easy to enforce them through system logins and the privileges attached to them (read only, read/write, system administration etc). However, it may be more difficult to automatically control at a systems level when it comes to creating documents, spreadsheets or emails. There is usually nothing to physically prevent anyone creating a document and calling it 'Annual Report 2007' or sending an email to the head of a neighbouring institution requesting a merger. These may be extreme examples that would be easy to spot as being bogus, but they serve to illustrate the point. The ability to prove its provenance and who was responsible for creating a particular piece of information could well be vital for protecting your institution's legal interests.

*"Provenance is the origin or source from which something comes, and the history of subsequent owners (also known in some fields as 'chain of custody')."*²

If this cannot be achieved by system functionality other possibilities may be to rely on the use of templates to which only relevant people have access, other types of authentication (such as biometric authentication), or the use of security controlled storage and publication facilities.

*"In information technology, biometric authentication refers to technologies that measure and analyze human physical and behavioural characteristics for authentication purposes. Examples of physical (or physiological or biometric) characteristics include fingerprints, eye retinas and irises, facial patterns and hand measurements, while examples of mostly behavioural characteristics include signature, gait and typing patterns"*³

The Dangers Of Over-Restricting Access

Of course putting too many barriers in the way of creating information may well be counter-productive and lead to user frustration and disengagement. Mandating that only the academic who authored a paper can deposit it in your repository may help ensure the integrity of the system's contents but is also likely to reduce the number of submissions from busy staff with little time or appetite for such administrative tasks.

The Benefits Of Unfettered Access

Much of the new generation of technology that is emerging is founded on the principles of collaboration and sharing. Social software applications such as wikis work on the basis that anyone who wants to contribute content is free to do so. It is for others to judge the quality of the

² Taken from the Wikipedia entry for Provenance on 20 July 2007
<http://en.wikipedia.org/wiki/Provenance>

³ Taken from the Wikipedia entry for Biometric Authentication on 20 July 2007
http://en.wikipedia.org/wiki/Biometric_authentication

information they create and to either embrace or ignore it as appropriate. The online encyclopaedia, [wikipedia](#) is perhaps the best known example of this.

This approach may well be highly beneficial where the objective is to get as many people as possible to contribute their ideas and opinions - especially in situations where everyone's point of view is likely to be equally valid. The important thing to ensure is that those wishing to make use of this information are aware of its mixed origins and the fact that it may represent opinions (as opposed to facts) based on differing degrees of experience and knowledge.

Creating Information In Appropriate Formats

When designing a new process or system which will create information it is advisable to think about the format in which it would be most appropriate to create it. Issues regarding its expected longevity, security and access concerns, potential for future reuse and its possible evidential value may all have a bearing. The question of information format is often overlooked in favour of a concentration on its content which can prove a costly mistake. Once again it is about ensuring that what you decide is fit for purpose. It is the equivalent of selecting the right tool to complete a manual task: a small hand-pushed mower might be fine for a garden lawn, but virtually useless for preparing a football pitch.

The various purposes for which email is often used represent an all too common example of widespread misuse of a format for creating information. People often treat it as the equivalent of a phone conversation and say things or express views which they would never ordinarily commit to paper. People forget that an email is a written record which may come back to haunt them. At the other extreme, a significant amount of formal business activity is often conducted via email with contracts being agreed and projects signed off. Whilst this may represent a perfectly legitimate form of business communication, it is also often the case that organisations fail to manage email appropriately, leaving potentially vital business records to languish unmanaged in an individual's inbox.

The World Wide Web has revolutionised our ability to quickly and cheaply publish information. When compared with the cost and time involved in manually printing and distributing a publication, it is little wonder that more and more institutions are choosing to only publish online versions of publications. But what if decisions are being made against the content of that publication which means it suddenly becomes necessary to know exactly what it said at a particular point in time some months or years ago? Unless your web content management system has sufficient capability to track changes and 'roll back' to how it appeared at a certain date it may be impossible to prove what your Research Ethics Handbook, for example, stated at the time a particular research project commenced.

An ever-increasing number of users are beginning to make use of externally-hosted social software services in which to create and store content. This could be a wiki being used to develop ideas within a project team, an online photographic service to store learning materials or even a 'virtual world' such as [Second Life](#) to create complex 3D models. Such technologies offer marvellous potential, but what would happen should the company providing the service suddenly go bankrupt or otherwise withdraw the service? Would you still be able to access the content you have trusted to it? There may also be questions to address regarding who actually owns the rights to the intellectual property of an object created in Second Life. Is it the individual user, the institution or Linden Labs who run this virtual world?

Lastly, there is the question of longevity and preservation. Much of the information we create will have a short lifespan of less than 5 years making questions regarding their longevity largely irrelevant. But a small percentage may need to be kept for far longer, perhaps for decades or even centuries. It may seem a real advance to scan your entire collection of paper files and store them on a handful of CD ROMs, but what if some of those records will need to be accessed in 70 to 100 years' time? In a few short years, it is more than likely that a CD-ROM drive on a new PC

will be as rare a sight as a floppy disk drive is today. Unless adequate preventative measures are taken those invaluable records may be as good as lost.

Capturing The Right Metadata

We may not always recognise it but metadata plays an invaluable role in allowing most staff to find and use information on a daily basis. Properties as simple as the title of a Word document or the name of the sender of an email in your inbox are all examples of metadata that we take for granted during our working day but would struggle to operate effectively without.

When designing a new process or system which will result in the creation of information, it is important to think through what metadata it may be required to create, not only to allow people to find it but for a host of other purposes. Whilst not all of the following types of metadata will always be relevant, it is useful to consider all possible aspects before deciding which are necessary and which can be discounted.

Metadata Types

According to the [MANDATE Toolkit](#) produced for JISC by John Wheatley College, the following main types of metadata can be identified:

- Bibliographic (e.g. "a picture of the Eiffel tower taken by Bob")
- Administrative (e.g. "taken on 19/04/2005")
- Legal (e.g. "all rights reserved")
- Preservation (e.g. "requirement to view as jpeg")
- Technical (e.g. "jpeg format" ; "85.8kb file")
- Educational (e.g. "an illustration of construction using cast iron"; "UK Education Level 11")
- Structural (e.g. "single file")

Whilst not a definitive list it does serve to illustrate the breadth of types of metadata to be considered. As ever, it is important to be selective, particularly if you are requiring users to input metadata manually. Wherever possible, systems should be designed to extract metadata automatically, thus ensuring its consistency and accuracy. If you are relying on users to add their own metadata, consider the level of burden this may place on the user and look for ways to ease it where possible, such as through the use of pick-lists rather than free-text fields.

Equally important is the need to ensure the consistency of metadata being applied to information shared across systems and processes. In an ideal world approved keywords would be taken from a single 'master' source and applied where necessary (for example, the list of budget codes being provided by the finance system, and staff names from the personnel database). If this isn't possible, it is important to at least achieve a degree of consistency regarding what metadata is captured for a particular type of information and in what format it should be expressed (all dates to be DD/MM/YYYY etc).

Active Use

Organisations are awash with information. Although the topics discussed in the previous section should help place some management controls around the creation of information, it is also necessary to think about how that information can and should be used. This is not to try to prevent innovation or stifle creativity, but to balance these positive aspects with the potential risks to the interests of your organisation which could occur as a result of the unfettered and uncontrolled use of information.

The active use phase of the lifecycle can best be described as the period during which information is in constant or regular use, primarily as part of the purpose for which it was originally created. There are no hard and fast rules for defining exactly what constitutes active use, but information which matches some or all of the following characteristics is likely to fall into this category:

- information which relates to a project or subject that is live and ongoing
- information required to perform a current function
- information still in draft status
- information that has been accessed and/or edited within the past three months, and
- the most current version of information that is routinely updated on a scheduled basis (for example the most recent version of an asset register which is only updated every five years)

Addressing the following questions will help ensure that your information is managed appropriately whilst in active use:

- Have you defined the purpose(s) for which your information can be used?
- Can your information be easily located and accessed?
- Do you know who needs access to your information?
- Is access to your information controlled?
- Is your information safe?

Define The Purposes For Which Your Information Can Be Used

The 2nd principle of the [Data Protection Act](#) states:

“Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.”

Failure to adhere to this principle risks separating the content of the information in question with the management and governance rules which have been agreed as being suitable for it. When dealing with personal data this could well damage the interests of the data subject (an identifiable living individual who is the subject of personal data) and in turn the reputation and legal standing of the organisation responsible. Without clarity regarding why that information was obtained, what it is to be used for and by whom, it is all too easy for it to be inadvertently reused in a way in which the data subject may not be comfortable with or which damages their interests. For example, an individual who gave information in confidence as part of a research project suddenly finding themselves publicly associated with those views.

But it is not just in relation to personal data that such issues need to be considered. The almost boundless potential to reuse information has been one of the defining characteristics of information technology in recent years. In the vast majority of cases the outcomes of such reuse will be positive and are to be encouraged. This could be the embedding of a digital photograph within the university website, the aggregation of existing statistics to undertake fresh analysis or making use of the content from a previous project proposal as part of a new initiative.

What is important is for there to be active and deliberate consideration as to whether any of the management controls associated with the original information either prevents or limits its potential reuse, or needs to be transferred to the new resource. For example, do the intellectual property rights associated with the digital photograph allow for it to be reused on your website? Does it contain images of individuals whose consent might be required? Will the credit for the picture be correctly associated to the original photographer or mistakenly attributed to the person responsible for scanning and manipulating it?

In order to achieve this, it is necessary not only to have defined what management controls are required for the information being created for its original purpose, but also to identify whether there are likely to be any issues associated with its reuse in the future. If not, great; but if so it is better to consider these issues in advance - or at least to flag that there may be issues to be addressed if and when this occurs in the future.

The issues raised in this section help demonstrate the intrinsic link between information and the processes which both create and rely upon it which is a recurrent theme throughout this infoKit.

Locating And Accessing Information

Being able to locate and access the information being created within your organisation in as quick and easy a manner as possible is clearly a vital issue. Failure to achieve this risks user frustration, wasted resources and potential difficulties in complying with legal requirements. It would seem logical that such factors are most likely to surface during the *active use* phase of the lifecycle for the obvious reason that this is the phase during which information will be most regularly accessed. However, it is also important that a longer term perspective is taken which also considers how access requirements may change over time. This is because information which is no longer being actively used on a daily or weekly basis is less likely to be found through proximity (i.e. appearing in your *recent documents*) and intuition and will be more reliant on the quality and logic of the measures you have put in place to describe it.

Unfortunately information description is not an area where most users excel. Information creators often resent having to manually add metadata to their resources and this needs to be borne in mind when designing or implementing any information system that is heavily reliant on user-generated metadata for content retrieval. Even if the completion of metadata fields is made mandatory there is no guarantee of the quality of data being provided with abbreviations, spelling mistakes and format inconsistency (ie how dates are expressed) dramatically reducing the quality and usefulness of the metadata being gathered.

In an ideal world systems should be designed to automatically generate as much resource discovery metadata as possible, either from information already known to the system (e.g. the user's name from the system login) or from the particular part of the process they are performing. Allied to this it is preferable wherever possible for any additional metadata required to be 'fed' from other systems which contain the definitive version of such information (for example providing staff names direct from the HR database). As well as ensuring the accuracy of the metadata such cross-system integration should also help facilitate cross-system searching.

Should this level of system integration not be possible there are still measures which can be taken to improve the ease with which information can be located and accessed. The [Managing Information to Make Life Easier Guide](#) has some good practical advice which you may find of use in this regard.

At the very least when creating a new system or process it is important to consider who else needs to know of its existence within the organisation and how they can obtain access to the information it produces. Individual 'silos' of information whose contents are known to and accessible only by a single member of staff is seldom helpful. Not only does it severely limit the usefulness of that information but may also make it difficult to provide an accurate and complete answer to a Freedom of Information request or other legal/regulatory discovery exercise. Perhaps the most overlooked example of such a silo is the average user's email inbox whose (considerable) contents remain accessible only by the individual user.

Who Needs Access To The Information?

Knowing who needs access to information and on what basis is of course closely related to discussions regarding how to locate and access it; but here we are dealing with the who and the why rather than the how.

Information delivered at the right time, in the right format to the right people is likely to be of far more use and impact than content which needs to be tracked down and liberated every time it is needed. This requires an accurate knowledge of your business processes and a clear understanding of how your information system is integrated within it. All too often the act of creating information is divorced from the business activity(s) for which it is required. This quickly creates monolithic silos of information with no apparent relevance to the functioning of the organisation.

The alternative is also true. One of the most common complaints heard of modern office life is that people are struggling to cope with ever-increasing volumes of information. Simply exposing staff to yet more information of limited or no value to their role is likely to be a futile and wasteful endeavour. Moreover, information overload is one of the main contributors to a lack of appropriate information management. Email is a classic example of this where, due to the excessive volume of messages received, users struggle to deal appropriately with messages as and when they arrive. So instead of either acting on the email and deleting it or filing it within the appropriate corporate space, messages tend to accumulate unmanaged within the user's inbox.

Restricting Access

It is also necessary to control access to information for reasons other than the convenience of the user. It is also required to protect the intellectual assets of the organisation, the personal data of stakeholders and the interests of third parties. Access to commercially-sensitive information and that given in confidence must be carefully controlled, as must personal information which is covered by the seventh principle of the Data Protection Act which states:

“Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.”

In practice it can be difficult to determine exactly who does require access to information, especially as this need can often be only temporary to fulfil a specific task. Once again a clear understanding of the business processes for which the information is to be used will be instrumental in ensuring an appropriate level of access control is maintained.

The results of such analysis will be required when formulating the access controls of a file plan within a shared document storage facility. Careful consideration is required to ensure that an appropriate balance is struck between open access and security to ensure that only the right people have access to the right information.

Semi-Active Use

Information is often only in regular active use for a comparatively short space of time. In due course its level of use will decline, perhaps because the information has been superseded or simply because the initiative to which it relates has itself ended. But this does not mean that its use, or indeed its usefulness have disappeared altogether. The information may still have residual value and be referred to on occasion for reference purposes, or may no longer have any informational value but still be required due to its possible evidential importance.

In many respects this represents the most problematic and potentially dangerous phase of all in the information lifecycle. This is because when information is in almost continual use this in itself often dictates its own management: we keep it close at hand and know instinctively where to find it, we know who we are working with and therefore who needs access to it and we know it has value because of its relevance to the task in hand. But when we have moved on to the next task and that peak of use begins to decline things become less clear-cut - a problem compounded by the fact that our interest and efforts have now been transferred to tackling the next task in front of us.

This is often the period during which people forget where the information came from, what its place in the process was or indeed why it was created at all. Such uncertainty often leads to the accidental breakdown of whatever carefully constructed management controls were put in place during the creation and active use phases. This can often lead to quite different and contradictory patterns of behaviour depending on the nature of the individual user. Where one member of the project team may come across project files from a long completed project and delete them as obsolete, five others may find the same files and each retain copies 'just in case'.

The following sections are designed to try to help you to steer through this grey period in the lifecycle and impose some structure on what can otherwise become the least well defined and managed part of the model:

- Do you know what information is being held and why?
- Do you know how long your information must/should be kept for?
- Can you assess the value of the information to the organisation?
- What are the most appropriate and cost effective means of storing information?
- Is your information safe?

What Information Is Held And Why?

It is important that your information management measures extend to semi-active and inactive information as well as covering information being used on a regular, active basis. As well as still having potential value this information, often sizable in volume, is still the responsibility of the institution and could be a potential liability if not managed appropriately.

There is a balance to be struck between sensibly relegating older information down the priority list whilst simultaneously avoiding the dangers of adopting an 'out of sight out of mind' mentality. Clearly you do not want to force users to wade through masses of less current information in order to find the information they need to perform the active task in hand. But equally it is important to retain contextual links between current initiatives and what has gone before and for users to know that the knowledge and accumulated wisdom obtained through previous endeavours may be relevant to their current work and is available to be learned from.

Defining The Journey From Active, To Semi-Active Use

It can be useful to clearly define the event-driven stage points which govern when different types of information move from an active to semi-active phase. For example, for project records 'project closure' may represent this trigger, or for student records it may be one year after the student has graduated. Once defined, such points should mark the formal dividing point between phases of the lifecycle and the trigger for a review of the management controls governing it.

The first such consideration should obviously be whether the information is still likely to be required now that its immediate *raison d'être* is at an end. The specific factors to consider in this process will be addressed in the following sections, so for now it is sufficient to highlight the importance of weeding information at this stage to ensure that only information required for a defined reason is being kept.

This review point is also the opportunity to consider the other management controls currently in place for the information and whether they are still appropriate. For example, do the security and access controls need to be adjusted, could the information now be stored elsewhere in less expensive 'offline' facilities, does the format the information was created in need to be changed to ensure it will be accessible in the future?

Retaining The Context

It is also worth considering what links may need to be established between this older content and any current or future work to which it relates. Will the way in which users search for information routinely cover both active and semi-active material? If so, does there need to be any kind of indicator to flag the different status of the information found?

Continued Maintenance

Although the kind of events we have discussed as marking the transition from active to semi-active use are an important stage-post, it is also important to bear in mind the need for continued review and maintenance of information throughout its semi-active life. Circumstances and requirements change over time. The sensitivity of information may decrease (or potentially increase), the rationale for continuing to keep it may change, or measures need to be taken to ensure its longevity. As a result, regular review of information held throughout the semi-current stage of the lifecycle is recommended.

How Long Should Information Be Kept For?

In an age where storage costs are relatively cheap (at least for electronic information), it can often be tempting to assume that the best route is to keep everything. However, this approach does lead to significant costs, even if many of them - such as decreased efficiency thanks to the amount of time taken to find the information required - are often hidden.

There are also considerable risks associated with keeping everything. All content held by (or on behalf of) an institution is potentially disclosable under the Freedom Of Information Act or as part of any other form of legal discovery exercise. Many organisations have found themselves in damaging or embarrassing situations thanks to the disclosure of information they still held, but had forgotten all about...

By using a consistent and objective set of criteria for determining how long your information should be retained, not only do you decrease the chances of important information being mistakenly deleted too soon, but you are also in a position to defend your inability to produce information requested under FOI.

The Drivers Governing Information Retention

There are a number of factors which can influence how long your information should be retained for. In broad terms, they can be divided into two main camps: internal and external factors.

Internal factors will primarily be determined by operational considerations, for example how long the information is likely to be needed both to fulfil the purpose for which it was originally created, but also for any secondary purposes. However, it is also important to consider the longer term historical perspective and whether the information in question is likely to be of interest to future generations as part of the documentary record of the development of the institution. The [Guidance on the appraisal of archival records](#) provides further information on making this decision.

External factors will be largely governed by legal and regulatory requirements. Many pieces of legislation will have statutes of limitations stated within them which helps define the minimum amount of time information covered by that legislation should be kept to ensure any subsequent legal challenge can be resolved.

"Statute of Limitation: 'A statute of limitations is a statute in a common law legal system that sets forth the maximum period of time, after certain events, that legal proceedings based on those events may be initiated. In civil law systems, similar provisions are usually part of the civil code or

criminal code and are often known collectively as 'periods of prescription' or "prescriptive periods"⁴

Although sometimes less clear cut, it is often possible to determine similar periods implicit within sector-specific regulation which can also be used as a guide.

Risk Management

It is perhaps worth remembering that all decisions regarding the retention of information is based on the management of risk. Even where limitation periods are clearly defined this only represents the minimum amount of time the information should be retained for - there may still be other factors which mean a longer period may be justified. Conversely, a shorter period could be considered where the volume of information covered is high and the perceived likelihood of it being required very low.

Assessing The Value of Information To the Organisation

As we have seen in the previous section, there will sometimes be clear and compelling external reasons for retaining information. However, where these do not exist it can sometimes prove difficult to assess the value of information to the institution with any degree of objectivity. Without a reasonably accurate estimate of its worth, it can then prove difficult to make any informed risk-based decisions regarding retention. After all, all storage of information costs money whether it is the fees associated with commercial storage of paper records, or the considerable overheads associated with ensuring continued access to electronic data. It is therefore important that you are sure that the value of the information to the institution justifies the cost of continued retention.

Defining Value

Unfortunately it is not always easy to quantify the value of information. If you decide to dispose of a text book you know how much it will cost to buy a replacement, but this is seldom true of internal information as its value is rarely defined in strictly monetary terms. The time required to recreate the information might be one measure, but in itself this does not help to define the likelihood of this scenario which will itself be dependent on the perceived value of its contents to the institution, its staff and stakeholders.

Thankfully there are some methodologies which are beginning to emerge which appreciate the intangible nature of the value of information and provide ways of quantifying their worth. The [espida project](#) at Glasgow University represents one such approach which may well prove useful for larger scale initiatives in this area.

A more basic 'ready reckoner' for deciding whether information is still worthy of retention is to ask yourself the following questions:

- Does it contain useful information that I or others will need to perform a specific and known task or role?
- Have you or a colleague referred to this information in the last 6 months?
- Is this the only place where such information is available?
- Is it likely that an auditor would wish to see this information?
- Are there legal or regulatory reasons for keeping this information?
- Is it likely that future generations are likely to be interested in this information as a historical record?

⁴ Taken from the Wikipedia entry for Statute of Limitations on 20 July 2007
http://en.wikipedia.org/wiki/Statute_of_limitations

If the answer to any of the above is 'yes' this may indicate that it is information that is worth keeping - at least for the time being. If the answer to all the above is 'no' it is unlikely that it is required and consideration should be given to removing it. Of course this can only ever be a rough guide and should be applied within the context of a risk management-based approach.

Appropriate And Cost-Effective Means Of Storing Information

As with all aspects included within the information lifecycle model it is important that the storage of information is fit for purpose. When in active use the prime determinant of fitness for purpose is ease of access: people want to be able to get hold of the information they require as quickly and easily as possible. However, when the frequency of use begins to decline so other factors also need to be considered.

Access will inevitably continue to be a factor - after all, there is seldom much point in continuing to store information if nobody is aware of its existence or knows how to find it. However, this consideration will inevitably be tempered by cost considerations. Near-line storage costs money, whether it is the costs associated with keeping paper records in prime office space, or delays caused by people sifting through unnecessary information to find the content they urgently require. This raises the question of what the alternatives may be and when it is appropriate to consider them.

Storage Options

For physical information, it may be worth considering moving semi-active content into off-line storage facilities which are usually located in cheaper, lower-grade accommodation and able to take advantage of economies of scale. Alternatively commercial storage providers can take away the need for onsite storage altogether - though at a cost and at a trade off in terms of speed and ease of access.

Crossing the boundary into the semi-current phase of the lifecycle might also mark the time to consider changing the format of information. Scanning can be an efficient way of reducing the physical footprint of your information but is not the quick and foolproof solution it can appear. Scanning is an expensive process and you want to be sure you are only scanning information that deserves the expenditure. There are also significant questions to be resolved regarding the management of the scanned copies and the longevity of the electronic, scanned versions.

For information that is born digital decisions regarding appropriate storage are less pressing, but do still exist. Some institutions employ email archives which automatically capture email and store emails within user accounts which are over a certain age. In such situations it is obviously important to consider carefully what this age should be and what the implications may be for information retrieval. Alternatively it is not unusual for users to create their own annual .PST files containing all of the emails they have sent or received during the year as a personal reference archive. It would be wise to consider the relative merits and potential risks involved in users adopting this approach and deciding whether to condone or condemn this practice.

Out Of Sight Shouldn't Mean Out Of Mind

It is worth remembering that the institution is responsible, and potentially liable, for all the information it holds. It is therefore important that wherever information is being stored, appropriate management controls are extended to it. Moulding boxes and unlabelled back-up tapes stored in a broom cupboard are of no use to anyone, but are a potential risk to everyone.

Is Your Information Safe?

The seventh principle of the Data Protection Act states:

“Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.”

This should act as a reminder that not only is it in the obvious interests of the institution to appropriately protect its information assets, but also potentially to a much wider set of stakeholders whose rights in this regard are enshrined in law. Clearly this is a pertinent issue throughout all phases of the information lifecycle, but is often perhaps most pressing an issue when the immediate use of the information diminishes and interest in it wanes. It is during this phase, as with so many other elements, that agreed management controls can inadvertently slip and good practice be forgotten.

The Overlooked Importance Of 'Good Housekeeping'

It is often the simple things which are overlooked but which can make the biggest difference. Although few of us ever manage to leave for home each night having left a completely 'clear desk' behind, users should be encouraged to at least ensure that confidential or sensitive material is locked away when not in use. Likewise, ensuring password protected screen savers are used, especially on PCs kept in open environments, is another simple yet effective preventative measure. Even such simple steps as ensuring that monitors being used in the processing of sensitive data cannot be read through a window or passing corridor can help.

Users should also be given guidance on what constitutes a good password (i.e. one which avoids proper names and includes numbers and symbols). When designing systems, consider whether to enforce the regular changing of user passwords - but beware that one unintended side affect of doing this might well be to encourage users to write their new password in obvious places rather than commit it to memory!

External Service Providers

There is an increasing trend for institutions and individual users to rely on online services provided by external companies to create and store information. This could be anything ranging from so called 'social software' services providing wikis, blogs and other online systems, to external hosts of online email and office applications.

It is worth giving careful consideration to the nature of the content users are entrusting to these services, and the guarantees you have regarding continued service delivery. Many of these companies are small with products in a perpetual state of beta development. It is inevitable in a competitive commercial environment that some services will be withdrawn and companies dissolved, potentially with little or no notice.

As such it would be unwise to rely on such services as the sole means of storing information considered to be of any real significance or value.

Final Outcome

The final outcome phase is, as the name suggests, the last phase of the lifecycle. As such it covers two different and diametrically opposed processes which together encapsulate the fate of all information: either its long term preservation or its deletion.

The whole lifecycle concept is founded on the importance of taking a comprehensive and proactive view about information management which seeks to look ahead, as well as dealing with the immediate challenges posed within any given phase. The issues surrounding the preservation of digital information illustrate the importance of this concept perhaps more than any other area due to the speed of technical change and the immense, sometimes unrecoverable, problems which can arise through attempting to deal with them retrospectively.

It is for this reason that there have been specific references to the challenges presented by digital preservation throughout the earlier sections of the lifecycle. However, it is in this last, final

outcome phase that we will explicitly address some of the main threats to ensuring access to electronic information in the longer term and the measures which can be taken to address these risks.

The two topics included in this phase cover both of the outcomes possible during the final outcome phase and include:

- How will you ensure continued access to the information?
- How is the disposal of information controlled?

Ensuring Continued Access To Information

Unlike paper, information stored in electronic media is inherently unstable and vulnerable to a wide range of risks, any one of which can threaten access to the content unless appropriate preventative measures are taken.

The major threats to the long term accessibility of digital information include hardware obsolescence, the incompatibility of software versions and media decay. Though it is impossible to define a specific time-span after which preservation issues are likely to become a pressing issue, it may be useful to consider 5 years as a general rule of thumb. For example, information that you know will only be required for less than 5 years is less likely to be affected by some of the preservation threats outlined above. Conversely, if you know the information being created will be of value for longer than 5 years, it is more important that these issues are at least considered. The table below is based on the assumption that the information in question will be required for longer than 5 years.

Although appropriate actions to counter these threats are likely to require large scale institution-wide measures, there are steps which can be taken whenever a new information system is proposed to help meet these challenges.

Measure	Purpose
Avoid proprietary data formats & systems	If the information being created is expected to be required for longer than 5 years careful thought should be given as to whether it is appropriate to rely on proprietary formats which may 'lock in' your data. This can make it difficult to perform future preservation actions and increase your reliance on external agencies over which you have no control.
Avoid storage on removable media	Removable storage media tend to age quickly, usually being replaced within a matter of years by new media with greater capacity, thus increasing the risk of hardware obsolescence. Removable media are also more likely to be stored inappropriately increasing the likelihood of loss or damage.
Consider when to upgrade software	Whilst it is not necessary to upgrade when every new software version is released, it is important to be aware of when your particular version will no longer be supported or will no longer be readable by subsequent versions and to take action accordingly.

Consider existing information when introducing technical changes	It is easy for decisions to be made on purely technical grounds without due consideration of its impact on existing information. For example, a decision to replace all PCs without an appreciation of the fact that a large volume of information still exists on floppy disks, the drives for which are not present on the new machines.
Consider the physical care of electronic storage media	Electronic storage media are often fragile and sensitive to fluctuations in temperature and humidity or to magnetic fields. Consideration should be given to where and how such media are being stored and they should be checked periodically to detect the first signs of deterioration before data is lost.

Controlling The Disposal of Information

Disposing of information may seem as straightforward a process as hitting the 'delete' key or finding the nearest waste paper bin. Unfortunately it may not always be a simple as that. It can prove more difficult than might be imagined to irrevocably remove electronic information to the degree required by the law. It is also a process which should now be as controlled and auditable as every other aspect of information management in order to protect the interests of the institution.

When Has Deleted Information Really Gone?

According to [guidance from the Information Commissioner](#) accompanying the FOI Act,

“Information located in desktop recycle bins is clearly subject to the FOIA as this continues to be held and is easily accessible. Once deleted from the recycle bin the information will also continue to be held unless the electronic record is completely erased from the computer system. Information in a deleted file or in a back-up, whether a server, disc or tape, may be regarded as being held by a public authority for the purposes of the FOIA depending on the particular circumstances of the individual case.”

It is therefore important that your deletion procedures are comprehensive enough to ensure that information you rightfully and lawfully wish to remove from your possession has actually been purged to the satisfaction of the above criteria.

It is possible to draw analogous conclusions for paper records - highlighting the importance of regular emptying of waste bins (particularly recycling bins) and the wisdom of providing confidential waste facilities and/or shredders where required.

An Auditable Process

To ensure appropriate levels of transparency and accountability it is considered good practice to document the disposal process and its outcomes. For example, to record what information has been destroyed, by what criteria it has been assessed as requiring destruction, on whose authority this has been carried out and to confirm the outcomes of the process.

Clearly any measures introduced in this regard should be proportionate and will require an analysis of risk. Obviously there is no need for the deletion of every email to be documented to this degree, but it may be wise to introduce a general policy statement which defines the types of emails which users can routinely destroy (spam, ephemera etc) and which should be subject to formal retention and appraisal procedures based on the significance of their content.

EMAIL MANAGEMENT

INFOKIT



www.jiscinfonet.ac.uk/infokits/email-management

Email Management

The rise and rise of email

Sending messages via electronic communication has a longer history than is commonly thought, pre-dating the internet and stretching back to the 1960s. However, it was with the advent of the World Wide Web during the 1990s that email as the business and social phenomena that it is today really took off. It is difficult to obtain accurate figures for the number of emails being sent at any one time but calculations in 2003 suggested a staggering figure of 31 billion emails were being sent each day with a prediction that that figure was set to double by 2006 (see the [Executive Summary](#) from How Much Information? 2003).

Regardless of the precise figures it is true to say that email has revolutionised business communication in a way second only to the introduction of the telephone and is indeed rapidly supplanting the phone as the method of communication of choice for many workers. It is now a common occurrence for an office worker to have to process in excess of 50-60 emails each day. Some of these may contain valuable information or represent important steps in the conduct of a business process; whilst others may be of fleeting or no use at all - or worse nothing more than spam designed to extort money or spread viruses. Email is now also integrated into other forms of business information - whether being used to transfer documents, co-ordinate diaries, or keep track of project milestones.

It is not hard to see why email use is so widespread. Its ease of use has helped form its own informal style which makes writing an email far quicker than composing a letter. The same message can be easily sent to as many people as you want at the same time and you can be sure that it will be received within minutes of sending it, compared with the days taken to receive post via 'snail mail'. And best of all of course it is free (at least so far as the end user is concerned). Whilst some of these advantages could also be claimed by the humble telephone, email has the added benefits to the sender of not requiring the recipient to be available at the time that he/she wants to communicate; whilst to the recipient they can choose to respond at the time that suits them as well as providing a useful written source to refer back to at a later date.

It's true that some new kids on the block are emerging which may over time challenge the dominance of email, especially the growing trend for 'instant messaging' solutions and [VOIP](#), but it will be some time before they topple email from the number 1 spot. The rise of wireless technology and mobile devices mean it is now as easy for users to send and receive email whilst out of the office as it is when sat at their desk - further adding to the convenience and usability of email and hence contributing to the ever increasing numbers sent.

The Risks Associated With Email

Unfortunately it is not all good news when it comes to email, and paradoxically many of the advantages listed in the previous section are also largely responsible for the considerable risks associated with its use.

Its ubiquity and flexibility mean that email is routinely used for an astonishingly wide variety of purposes, some of which are outlined in the table below

Table below - Range of functions email is regularly used for

Sharing information	Sharing documents	Asking questions
Requesting information	Planning social events	Agreeing a course of action

Sharing jokes/gossip	Holding discussions	Swapping contacts
Planning business meetings	Confirming agreements	Assigning tasks

This mixture of formal and informal, business and social, serious and frivolous is a dangerous mix. The eyes of the law may be unable or unwilling to distinguish between them leaving every single email sent or held by your institution as part of its auditable information holdings. With all colleges and universities now subject to the [Freedom of Information Act](#) the question staff need to ask themselves is: 'would I be happy for the contents of my email to be printed in the local newspaper'? The answer is likely to be a resounding 'no'. This is because people have become accustomed to treating emails as ephemeral without regard for the evidential trail they leave behind. There are countless examples of users who have fallen into this trap only to find their flippant, off the cuff remarks used against them as evidence of libel, discrimination or abuse.

Nor is this a risk faced solely by the individual staff concerned. The institution itself may well find itself liable for the transgressions of its staff - especially if it is unable to demonstrate that it is taking an active approach to encouraging good practice and managing email use.

The ease of email creation and distribution, combined with the sheer volume of messages that staff are expected to deal with also leads to inevitable problems. Messages containing sensitive content are all too easily sent to the wrong person who just happens to share a similar name to the intended recipient, whilst confidential information is often to be found inadvertently buried at the bottom of a long chain of forwarded messages.

Without regular, ongoing management by the user their email account will rapidly become an untamed and apparently untameable monster. Inboxes containing literally thousands of messages are not uncommon and many people have developed a way of working which relies on the kaleidoscope of information their inbox contains as an apparently indispensable 'electronic memory'. Whilst there may be some value to the user in this approach (though probably less than they imagine) it also results in considerable costs and risks to the institution. As well as the dangers resulting from inadvertently keeping 'dangerous' information, it is also often the case that information of value to a number of functions within the institution remains locked away within this inaccessible data silo and reliant on the vagaries of individual practice for survival.

Creation

Both email as a format and the functionality of the applications used to create them contributes largely to the problems associated with their management. Most aspects of email technology and functionality are weighted in favour of the sender and as a result work against the interests of the recipient. For example the ease, speed and cheapness of their creation and distribution mean little or no forethought or consideration is required. There are no practical barriers or costs associated with creation which might cause the potential sender to pause and think twice before creating yet another message.

Until recently this has seemed a relatively trivial issue. Users may individually struggle to cope with the volume and variety of messages they receive but the associated costs and risks to the institution as a whole were largely ignored. Now, with email servers containing terabytes of data the costs associated with storage and maintenance are no longer trivial. Furthermore institutions are beginning to realise the hidden costs and dangers associated with uncontrolled email creation - not least the risk of dangerous and damaging information coming to light as part of a response to a Freedom of Information Act request or other legal discovery exercise.

Many institutions are rapidly coming to the conclusion that email management can no longer be left to individual members of staff to perform on a 'best efforts' basis and that a more proactive and co-ordinated approach is needed. The purpose of this strand of the Managing the Information

Lifecycle infoKit is to outline the main elements which need consideration as part of such an approach. In particular looking at how a combination of three main elements; technology, policies/procedures, and user training need to be considered in unison to achieve an effective, institution-wide response.

The contents of this section build on and augment the information provided in the Information Lifecycle - Creation strand and should be considered in this light. What this section attempts to do is build on the general good practice guidance on information creation covered previously and look specifically at the additional requirements for creating good emails.

As such it will be of use to those tasked with managing and maintaining email services within the institution and those with an interest in the management of information and records.

The topics covered within this section include:

- Ensuring appropriate email use
- Encouraging staff to create fewer emails
- Encouraging staff to create better emails
- Email 'disclaimers'

Ensuring Appropriate Email Use

As we have already seen, the flexibility of email has led to a user culture where email is routinely used for a variety of formal and informal purposes. It is therefore vital that the institution clearly defines what is and isn't 'acceptable use' of email and that users are informed of the distinctions.

Appropriate Use Policy

Formulating an email appropriate use policy provides an essential cornerstone of this strategy. Without a clear definition of what is and isn't acceptable the institution will not be able to demonstrate that responsibility for any breaches of the law rests with the individual and not the institution. It is also less likely that the institution will be able to take punitive measures against any staff found using email inappropriately.

Some categories of inappropriate content/use will be easier to define than others. The table below includes categories of email which will need consideration when formulating an appropriate use policy - whether they are deemed 'inappropriate' will, in some cases, be dependent upon local circumstance. As the table below makes clear, inappropriateness might equally be judged according to whether email is considered the safest, most appropriate format for transferring what is actually perfectly 'legitimate' content.

Table below - categories of email content which may be deemed inappropriate

Category	Examples
Malicious	Viruses, worms, Trojans etc.
Illegal	Pornography, terrorism/extremism, libellous
Offensive	Sexist, racist, harassment, bullying

Sensitive personal data	Disciplinary matters, health/medical information etc.
Commercially sensitive data	Financial information, contractual negotiations, intellectual property
Personal use	Online shopping, gossip, arranging social life, etc.

Making Staff Aware

It is an important first step to formulate what is and isn't acceptable use into a policy, but this alone is not sufficient. The most obvious additional requirement is that staff are informed and regularly reminded of the policy and its contents. The policy should be endorsed by senior management and distributed to all users bearing this official endorsement. Including it as part of induction packs for new starters will ensure all new staff also receive it. Its content should form part of any IT user training (e.g. as part of Introduction to Outlook courses) and links to it should be provided from the institution's webmail service home page and the intranet.

Enforcement

Breaches of the policy should be stated as a disciplinary offence and potential grounds for dismissal within staff contracts. Consideration should also be given to internally publicising breaches of the policy and any measures taken as a warning to others.

Encourage Staff To Create Fewer Emails

Given that a large percentage of the emails received by staff within your institution will have been created internally, reducing the number of emails individual staff send will subsequently reduce the number of messages all staff receive and need to manage. This will not only help reduce the overall volume of network traffic and decrease the chances of mistakes through user-error, it will also increase the overall efficiency of your institution. Many users will instinctively break off from the task in hand when notified that a new message has been received, thus breaking their train of thought. Also, if you assume an average of 2 minutes is spent reading and responding to each message, multiplying that by the average number of messages received and then by the number of staff in your institution it is possible to quickly arrive at a frighteningly high staff-costs figure.

Providing And Promoting Alternatives

In order to try to wean users of sole reliance on email it is necessary for the institution to provide and promote alternatives. That way email can be seen as representing just one tool amongst many at the user's disposal for use only when it makes sense to select it. Remind users that one quick phone call can save a dozen emails when trying to arrange a meeting and support this by ensuring that the internal phone directory is easy to find and up-to-date and that staff have access to modern phones which can store frequently used numbers etc.

The institution should also ensure efficient use of its intranet to distribute 'all staff' information, perhaps making use of RSS feeds to notify users of updates and changes. It should also ensure that all staff have access to shared file areas to prevent the need to rely on email to share documents (this also has additional information and records management advantages explored in [version control](#) from the Records Management strand).

Promoting Good Practice

A combination of documented procedures and user training will make a significant difference. These should not only cover when not to use email as outlined above, but also more detailed guidance on thinking carefully before selecting 'Reply All' or when sending emails to large groups of users. The institution should ensure that it practices what it preaches in this regard as the high volume of 'All staff' emails used to transmit information of use to only a very small, easily identified, group of users is often a common culprit!

Some organisations have gone even further and instituted regular 'no email days' when it is forbidden (or at least strongly frowned upon) to send or respond to internal emails. Such initiatives, even if promoted as one off events can help raise the profile of the problem, remind users of the alternatives and help them recall the advantages of an un-interrupted period of work.

Publishing statistics on the volume of emails sent by the institution's servers each day/week/month and setting a reduction target can also be an effective way of raising awareness - especially if accompanied by a small prize for the team or department which manages to meet the target figure first.

Improving Your Email

There is little that can be done from the technical or system perspective to encourage staff to create better emails. Any improvements in this regard are likely to be largely dependent on the same blend of procedures and user training referred to in the previous section.

Once again, the focus is on changing the behaviour of the sender to make life easier for the recipient and thus helping to initiate a virtuous circle of improved management. Poorly drafted emails described by unhelpful (or absent) titles and accompanied by indiscriminate use of message status indicators are not only annoying to receive but add considerably to the daily burden of trying to manage email. They also increase the risks of damage to the institution's reputation and legal interests through the amplified likelihood of mistakes caused by poor management and the transmission of inappropriate material.

Titles & Other Metadata

The only user generated metadata routinely added to an email is the subject heading or title. As such it is important that the user is made aware of the value of attaching good, clear and unambiguous titles to all their messages. Ideally the title should be clear enough for the recipient to know the basic content of the email and its context prior to opening the message. Particular attention should be paid when the content of a thread of messages changes over time and starts to have little or nothing in common with the original title. The default options within your email application should be checked to see whether it is possible to prevent messages being sent where the subject header has been left blank.

The use of message status indicators can be helpful to provide an immediate indication to the recipient of whether an email is urgent or of low importance. Users should be encouraged to use these sparingly (especially the 'Urgent' indicator) to preserve their impact. The default system configuration should make both buttons readily available from the application toolbar.

Content

Users should be encouraged to stick to one main subject within each email, rather than using one message to cover a wide range of topics. Otherwise not only does it become impossible to accurately express the nature of the content in the subject heading, but it is also difficult for the recipient to apply appropriate management controls to the email (into which folder should it be stored, how long should it be kept, etc).

Users should also be trained to avoid the growing tendency to use abbreviations and 'text message' language within emails. Such shorthand can easily cause confusion and mis-

interpretation. Likewise users should be made aware of the benefits of using objective, conversational English and avoiding subjective comments or jokes which can be easily misconstrued.

Email Disclaimers

The value of email 'disclaimers' attached to every email sent by the institution and specifying the conditions under which the message has been sent and should be treated is hotly contested. On the one hand their legal status and the level of protection they offer is at best limited (if not non-existent), and yet on the other hand virtually every organisation - including legal firms - seem compelled to include them; suggesting they must have some value.

The Case 'For' Disclaimers

Thanks to the legal concept of 'vicarious liability' the institution is responsible for the actions carried out by its staff - hence the whole reason for institutions to be concerned by how their staff use email in general. However, the institution may also be held liable by a recipient who believes they are communicating with a genuine member of staff even if they are not. A disclaimer can help clarify the legality of an email and the way in which its contents should be interpreted.

The Case 'Against' Disclaimers

Most disclaimers are poorly drafted, inappropriately situated within the message and used indiscriminately - thus removing most, if not all, of their effectiveness.

For example there is little point attaching a disclaimer to the very bottom of your emails (where the vast majority are situated) which states words to the effect of "if you are not the intended recipient of this message please do not read it". Likewise where such text is added to emails sent to JSCMail email lists where the message is then sent indiscriminately to hundreds of recipients.

Poorly drafted disclaimers will not only remove any last remaining vestige of legal rigour, they may also serve to portray a negative image of the institution as either being overly bureaucratic, naive or inept (or all three!).

Institutions are advised to seek their own legal advice regarding the pros and cons of disclaimers and when drafting the text of such a statement if they do choose to use one.

Some useful and entertaining non-legal advice on this topic is also available from the [University of Dundee](#)

Active Use

The potential range of issues emerging out of the active use of email are widespread and complex, including technical issues surrounding online security and legal issues relating to the monitoring of users online activity. Thankfully the focus of this resource is specifically on the information itself, which in this strand means the actual emails which have been created and are now in 'active use'. Inevitably any discussion of the active use phase of the email lifecycle will have to dip into these broader topics because of the impact they will have on the way in which emails are used and managed. However, it should be noted that the focus of the guidance included within this phase of the infoKit unapologetically remains the management of email itself with only superficial and passing reference to these broader topics where specifically relevant.

The contents of this section builds on and augments the information provided in the Information Lifecycle - Active use strand and should be considered in this light. What this section attempts to do is build on the general good practice guidance on information creation covered previously and look specifically at the additional requirements for managing emails.

As such it will be of use to those tasked with managing and maintaining email services within the institution and those with an interest in the management of information and records.

The topics covered within this section include:

- Monitoring email use
- Remote/home use of email
- Outsourcing your email provision
- Email security
- Making best use of your email application

Monitoring Email Use

As in most areas of institutional life it is comparatively easy to draft and approve policies, such as the Email Acceptable Use Policy mentioned in the previous section. However, it can often prove far harder to actually ensure that the policy is being adhered to. It also raises the question of what the institution will do if and when it discovers user activity which is in breach of its policy. Thanks to the concept of vicarious liability outlined in the section of email disclaimers the institution is liable for the actions of its employees. In legal terms having a policy which is generally ignored and widely flouted is unlikely to be considered much of a defence against any claims of culpability.

However, the institution must also ensure that any actions it takes to monitor the email activities of its staff are also legal and conform to all relevant legislation. Otherwise not only will the institution find itself unable to take appropriate measures against any users found breaching the rules, but may even find themselves on the wrong side of the law with action taken against them accordingly. The key pieces of legislation to consider in this area are:

- [The Regulation of Investigatory Powers Act 2000](#)
- [The Human Rights Act 1998](#)
- [The Data Protection Act 1998](#)

The [JISC Legal Information Service](#) contains specific guidance relating to the monitoring of electronic communications as well as more general information about such. These include:

- Interception & Monitoring Law ([webcast](#))
- Interception & Monitoring Law ([transcription](#))
- Interception & Monitoring Law ([FAQ](#))
- [Data Protection Act 1998](#)
- [Monitoring Internet Use](#)

As stated in all of the above sources, these are intended as legal information only and it is advised that institutions seek their own legal advice in relation to specific issues.

Further information is also available from the [Office of the Information Commissioner](#)

Remote/Home Use Of Email

Email use is no longer tied to the desktop and restricted to the office. A host of technologies now make it possible to create and receive messages whilst at another location or in transit between locations. These are all positive developments that have done much to increase the productivity of users; but at the same time it is important that the risks inherent in such flexibility are

recognised and addressed. The institution should seek to ensure that same level of management control is extended to the active use of email where ever and how ever it is being used.

It is important that remote and/or home workers recognise that the emails they work with 'off campus' are subject to exactly the same policy framework as all other institutional emails. This should be communicated to any users affected as part of the terms and conditions of working remotely.

It will prove easier to retain a consistency of approach to email management, regardless of location, if staff email is configured on an IMAP rather than POP basis. Use of IMAP ensures that all messages contained within a user's email account are stored centrally on the institution's servers and are only retrieved when required. A POP-based email service downloads messages for storage on the individual user's machine resulting in a range of potential management problems as indicated in the table below:

Table outlining the management problems associated with POP-based email provision

Issue	Implications
Information loss	Unless copies are also being retained on the server any fault or theft of hardware could result in valuable information being irretrievably lost
Information security	Loss or theft of hardware could result in sensitive or confidential information falling into the hands of 3rd parties. There are countless examples of laptops containing such information being stolen from cars, hotel rooms, conferences etc.
Legal discovery	Emails stored locally may not be located or accessible if required as part of a legal discovery exercise or request for information
Inconsistent retention	Emails stored locally are less likely to be retained or destroyed according to pre-defined business rules
Gaps in the evidential record	Emails stored locally will not be accessible to others and important information may appear to be missing from the information associated with a particular process or transaction.
Preservation	Emails stored locally are less likely to be subject to any institution-wide preservation activity, thus increasing the chance of them becoming inaccessible over time

Those using mobile devices such as Blackberries should ensure that access to the device is password controlled. They should also be encouraged to resist the temptation to adopt a 'text language' approach to creating emails on such devices. Abbreviations and use of slang are open to mis-interpretation and are not appropriate for what may form part of an official business record.

Outsourcing Your Email Provision

Trinity College Dublin hit the headlines earlier this year with the announcement that they are to outsource their entire institutional email service to Google. Other institutions seem set to follow suit and realise the significant cost savings which may go with the outsourcing of your email service.

It is outside of the remit of this resource to offer any judgement on the nature or degree of financial savings that can be realised, or the technical implications which are associated with making such a move. Instead what follows are some aspects to consider prior to embarking on this course of action which may affect the way in which your institution is able to manage the emails it uses.

It is important that the institution realises that although it may be outsourcing the technology and service provision it cannot simply divest itself of responsibility for email management by outsourcing its liabilities to a 3rd party. The concept of vicarious responsibility will still apply and the institution is still liable for the emails created or stored by its users. Recognition of this fact colours many of the remainder of the issues to be considered, revolving as they do around the need to continue to meet these responsibilities even when you are not in day to day control of service provision.

Consideration should therefore be given to the following issues:

- Are you aware of the type and nature of personal data collected by the service provider about your users? Is this in line with your legal responsibilities, is it ethically defensible and has it been communicated to your users?
- Are you aware of who will own the copyright contained within the messages stored by the service provider? Have you considered the implications if copyright is to rest with the service provider?
- Are you aware of and comfortable with the level of back-up and disaster recovery measures being offered for your email?
- Are you aware of how long the emails created or received by your users will be routinely retained by the service provider?
- Are you able to define and enact your own retention actions on the emails stored by the service provider according to the messages content?
- Are you comfortable with the level of preservation measures available and their ability to provide continual access to emails for long periods of time (for example over 50 years)
- Will you be able to extract and move all of the emails your users have created at any point in the future to another service provider (or back in house)?
- How quick and easy will it be for the institution to update or remove a user's system privileges?
- Have you considered how this hosted service will interact with other institutional systems? How easy will it be for users to associate the contents of emails held by the service provider with related information held within the institution? What impact may this have in terms of resource discovery and management?

Careful thought should be given as to whether outsourcing is the right move for the institution if the proposed service provider is unable to provide satisfactory answers to any of the above - regardless of any perceived immediate technical or financial benefits.

Email Security

The question of email security is addressed within this resource from a broadly non-technical perspective and instead focuses on the role of the user in this regard and the role they must play in protecting the security of the emails they create and use.

Perhaps rather strangely one of the key messages that users should be supplied with with regards to email security is that email is inherently insecure. Unless specific measures have been

taken to provide a secure, encrypted system users should be made aware of the limitations of current security provision. Such technical limitations may have a bearing on the institution's acceptable use policy by prohibiting the use of email to transmit sensitive or confidential material due the institution's inability to provide appropriate levels of security for such information.

Passwords & User Behaviour

Users should be provided with guidance as to what makes a good or bad password and encouraged (if not forced) to change them regularly. If no password is required to access a user's email account once they have logged on to their machine they should be encouraged to make use of password controlled screensavers, especially if working in an unsecured area. Password-controlled access should also be enacted on any mobile device used to send or receive email.

Institutions need to be mindful that whilst the majority of their staff are likely to be experienced email users, there may also be a small number who are using it for the first time and who are less aware of the dangers posed by viruses, spam and email 'phishing' scams. Care should be taken to ensure that appropriate guidance and awareness training is provided for such 'novice' users.

Account Maintenance

Institutions should ensure they have well established procedures for terminating access to a user's accounts when they leave the institution. This is particularly important now that virtually all institutions offer a webmail service which would allow the former member of staff to continue to access and use their account even without access to the desktop email application.

This of course raises the question of what should happen to the contents of a user's email account when they leave the institution. This subject will be addressed in the Managing Email Retention section of this resource.

Making Best Use Of Your Email Software

Most email applications contain a significant amount of functionality which can be routinely employed by users to better manage their inbox. By doing so they not only help lessen the burden of trying to keep pace with their email, but by extension they also help reduce the institution's exposure to risk by decreasing the likelihood of inadvertent user error. Unfortunately users are seldom made aware that such functionality is available to them or provided with training in its use.

The following table demonstrates the range of 'inbox management' functionality available within Microsoft Office Outlook 2003. Functions may vary, or not exist within other applications.

Table illustrating email application functionality and its use in email management

Function	Use
Changing the colour of messages addressed solely to the recipient	Makes it easy to see at a glance which messages are addressed solely to you (often an indicator of messages requiring more immediate attention and action).
Adding 'flags' to messages from certain people or containing certain characteristics	Useful for quickly sorting, prioritising and arranging messages.

Turning off the new message notifications	Prevents users from being constantly disrupted and diverted from their work every time a new message is received.
Creating and naming sub-folders to match your main shared filing system	This makes it easier for users to manage their email in tandem with the other information to which it relates. It also makes resource discovery across systems easier.
Create rules to automatically move emails matching certain criteria into the appropriate sub-folder	Acts as a useful default pre-sorting of content. It also helps increase the obvious value of ensuring emails have accurate subject headings.
Ensure emails are removed from your 'Deleted items' folder on application closure	This ensures that emails intended for deletion are removed from the user's application and do not inadvertently remain.
Save replies with the original message	Can be useful for ensuring that both sides of a transaction (i.e. messages both sent and received) are captured and managed as one.
Out of office assistants	An important requirement to ensure compliance with the FOIA. Enacting an out of office alert which includes an alternative contact point will 'stop the clock' of any request received.

The [Managing Information To Make Life Easier: A Guide For Administrators](#) resource provides further practical tips to help users manage their email more effectively.

Semi-Active Use

Email is not only a quick, convenient means of transferring ephemeral information. Emails can be, and often are, formal business records which provide evidence of important transactions. Most of the guidance relevant to the semi-active phase of the lifecycle reflects this need to manage emails as records. Although a consideration throughout all phases it is largely in this semi-active phase, after their initial reason for creation and active use have declined, that the majority of these factors will come to light.

As the active use of the email declines so too often will the interest of the user. This can lead to a management vacuum which in turn leads to inconsistent measures being applied, or worse still no measures at all. It is important that the institution takes action to fill this void from the centre, thus protecting its interests and helping the user to operate effectively.

The contents of this section build on and augment the information provided in the Information Lifecycle - Semi-active use strand and should be considered in this light. What this section attempts to do is build on the general good practice guidance on information management covered previously and look specifically at the additional requirements for managing emails.

As such it will be of use to those tasked with managing and maintaining email services within the institution and those with an interest in the management of information and records.

The topics covered within this section include:

- Identifying emails as records
- Managing emails as records
- Managing email retention
- Managing email retention in context
- Finding emails

Identifying Emails As Records

Given the tremendous volume of emails sent and received by the institution each day it is neither practical nor desirable to manage each and every one as a formal business record. The trick is to be able to identify and capture that small percentage of emails that need managing as records - to separate the wheat from the chaff.

This will depend in part on the institution having formally defined what constitutes a 'record'. Further information on what properties and characteristics define a record are included in the Records Management - What is a Record? Section . The whole records management strand of this resource is relevant to this area in terms of identifying the specific qualities associated with records and the management controls required to preserve them.

It is also important that users are given clear, simple guidance on which of their emails might constitute records and require handling accordingly. This should include both categories and possible examples. For example:

Category	Example
Formal agreements	Approval of contracts, project plans, policies, etc.
Decisions/confirmation of actions	Approval to spend money or to carry out a particular activity
Confirmation of completion	Project sign off, receipt of goods, etc.

Next Steps

It is one thing to equip the user with the ability to identify the records contained within their email, but this is of little consequence if they are not also given the means to act accordingly. For those emails which are identified as being records it is important that they are formally recognised as such and managed in context with the other records to which they relate. This is likely to require the transfer of the email record from the user's inbox to whatever facility is being used to store and manage all other records within the institution. This may be either a shared file server, document/records management system, repository or collaborative technology such as Microsoft Office Share Point. It could even mean printing out the email and managing it as a hard copy record if no suitable electronic facility exists.

It must be made as easy as possible for users to transfer email records to such systems so as not to erect any unnecessary barriers to this process. The email records should be transferred to the appropriate area of the record-keeping system and then managed in a consistent manner to all

other corresponding records. In this way the email record will be managed appropriately according to its content and not based on the fact that it happens to be an email.

Managing Emails As Records

The transfer of email records to the appropriate recordkeeping system as described in the previous section is a critical stage in the process. However, the simple act of transferring the email record is not in itself sufficient to ensure the preservation of their evidential and informational value. Everything possible must be done to ensure the maintenance of the email's record-like properties and characteristics during and after this process. These properties include the following (all of which are explained in more detail within the [Records Management strand](#) of this resource) Authenticity, Completeness, Reliability and Fixity.

Authenticity

In order to demonstrate the authenticity of the email it is important that all sender and recipient information is carried over with the email record - including all parties receiving the email as a carbon copy (CC) or blind carbon copy (BCC). Some legal opinion also asserts that an email can only be considered a legal record if the author has manually typed either their name or initials at the end of the message. Reliance solely on a name which is automatically included as part of an email signature may not be regarded as sufficient in this regard.

Completeness

The completeness of the email as a record can only be assured if all component parts of the email are transferred and retained together as a single record. This includes the text contained within the email itself, the transmission data included within the email 'header' and any attachments originally associated with the message.

Reliability

As with all records it is largely up to the original author to ensure that the contents of the email record are accurate. However it is also important to be confident that nothing has changed within the content of the email record during the process of transfer to the record keeping system. This may be especially relevant if the format of the email is being changed during this process (i.e. from its native Outlook Message Format or HTML into a text file).

Fixity

It is important to ensure and be able to demonstrate that no element of the email has been or can be altered in anyway after being declared as a record. This includes changes to the content, but also to the transmission data and the content of any attachments transferred with the original message. This may be variously achieved by altering the properties of the file to a 'read only' status, or modifying the permissions within the specific area of the record keeping system to prevent further amendment.

Managing Email Retention

"Does your organisation retain all your email forever? Congratulations. You are a disaster waiting to happen." (Amacom, 2003)

The costs and dangers associated with keeping too much information, and the risks of not retaining the right information have already been covered in the [Records Management strand](#) of this resource. The same drivers apply equally to the retention of email and yet as a rule it is an area that if not ignored completely is usually handled inappropriately.

By What Criteria Should Email Retention Be Decided?

The only restraint usually placed on the retention of email is the imposition of pre-set storage quotas on individual user accounts. The intention of such limits is to prevent the unlimited accrual of email but adopting this approach does little to achieve this. When confronted with an 'inbox full' message most users will simply 'archive' a vast chunk of their messages and store them on their desktop as .pst files. In this scenario not only do the emails still remain, but they are now contained within an unmanaged and inaccessible local silo.

Alternatively users will often simply select those emails with the largest attachments that they have no immediate use for and delete those in order to reduce their account size back to a 'legitimate' level for a few days. Both of these represent retention management based either on file format or file size and neither pay due attention to the email's content: the property which should be the key determinant of its retention.

Retention Based On Content

It is one thing to state that email retention should be determined by its content, but quite another to enable this. Firstly it assumes that you have a retention schedule in place which defines the appropriate [retention period for records](#) of various types. Secondly it relies upon each user being able to quickly and easily make the right decision regarding the content of an email and how long it should be retained for - no easy task given the vast number they receive each day.

Separating The Wheat From The Chaff

The process of separating email records from email ephemera as outlined in the previous section has an important part to play in making this task more manageable. One way of doing this is to consider introducing an automatic deletion policy for all emails older than a certain amount of time (perhaps 90 days). After this time (by which any initial informational value is likely to have expired) the email is routinely removed from the user's inbox and permanently deleted. This relieves the user of the need to concern themselves with managing the ephemera - leaving them to concentrate on what they must do with the small proportion of emails which should be managed as records. This policy is not without risks, dependent as it is on the user to identify which emails are records and to categorise them according to their content to ensure their appropriate management. Being forced to choose what emails they must keep as opposed to which they should delete is a subtle, yet profound, change to the culture of email use and the role of the user within it and is not something to be introduced lightly or without due prior training and awareness raising.

Managing Email Retention In Context

What we are trying to achieve in this and the previous section are ways of ensuring that email retention is managed in the same way as the retention of any other type of record. This is why the sections of records retention are so relevant to this topic. At the same time we cannot ignore the fact that the volume and nature of email as a format adds the difficulty of achieving this. Routinely removing ephemera as previously described can be successfully adopted as the first stage of the process. The next step requires the user to transfer their email records to whatever repository is being used to store the other records to which they relate (for example shared file server, document management system etc).

Ideally users would do this as and when such email records are identified. That way the email records they possess become part of the institution's 'official' shared and managed information holdings as quickly as possible. In reality, however, this may prove unworkable where large numbers of email records are being created or received by busy members of staff. In such circumstances an acceptable compromise might be to encourage transfer of all such email records at defined points in the process. These may include official project gateways and review points or at project closure for smaller projects, completion of a tender process or of the entire

contract to which it relates etc. The Semi-active use - Do you know what information is being held and why? section of the Information Lifecycle strand of this resource provides further information about how to identify these points in the lifecycle of information - reflecting as they do the dividing line between active and semi-active use.

By encouraging users to create email folders which mirror those of the main record/document filing system as suggested in Active Use - Making best use of your email application section it should prove easier for the user to quickly and easily identify the correct folder for these emails to be transferred to.

What Happens When A Member Of Staff Leaves?

If the institution has adopted the measures outlined within this resource it is to be hoped that a departing member of staff's email account should only contain a relatively small number of messages relating to current activity. These should be arranged in such a way that it is then a comparatively easy job to transfer them over to the respective folders to which they relate in the main shared file area as part of their hand-over activities.

Unfortunately what institutions will also often find are that the accounts of departing staff contain hundreds if not thousands of random, unmanaged emails relating to a wider range of topics: trivial and important; current and completed. In this scenario the institution has three basic options: to go through and sort them out individually; to keep them all or to destroy them all. Which of these is adopted will depend upon the number of emails in question, the seniority and importance of the member of staff concerned and the degree of risk it is believed retention of the total collection involves. If the institution does decide to retain all messages when an employee leaves it is suggested that a policy is enacted whereby any of their emails then subsequently accessed are transferred into the appropriate 'corporate space' and that after an agreed period of time (3 years?) the remainder of their emails are permanently deleted.

Finding Emails

As we have seen, emails can often contain valuable and important information, they can also act as vital links in the chain of evidence required to justify a course of action or protect the institution's legal interests. Any of this is only possible if all relevant emails can be identified and located when required. The focus during this semi-active phase of the lifecycle is therefore less on ensuring that the individual user can navigate their emails effectively and more on the issues presented by the need to locate emails from across the entire institution in response to an external demand. That said the ability to meet these demands as an institution will largely be dependent on the actions of individual users and the way in which they create, name and manage their messages as described in the creation and active use phases.

The Advantage Of Central Storage

Any form of external request for information held by the institution, be it an FOI or Environmental Information Regulations Request, Subject Access Request under the Data Protection Act or any other type of legal discovery exercise may well cover emails received by staff across the length and breadth of the institution. This is one of the reasons why the use of IMAP over POP as the method of retrieving emails is recommended - see Active use - Remote/home use of email for further details. Central storage of emails at least provides the potential for cross-server analysis and resource discovery using any one of a number of commercial email management or 'archiving' software. Emails stored locally on individual PCs, laptops or external storage media will not be covered and therefore may not be found during any such discovery exercise.

It is important that any such analysis of staff user accounts is conducted in accordance with the law, as outlined in the Active use - Monitoring email use section.

It is more likely that any discovery exercise will relate to a specific topic or event ("I would like to see all information relating to topic X", or "there is a court case pending relating to the patent of

research project Y") rather than just to email specifically. It is for this reason that we suggest managing email alongside all the other information to which it relates. That way all information relating to topic X or Y will be located and easily retrieved from one place.

User Behaviour During A Legal Discovery Exercise

Despite these measures it is inevitable that individual users will hold emails and other information which relate, no matter how tangentially, to the topic under investigation. Any staff who are believed to have played a role in the process or to have received information relating to it should be immediately and explicitly instructed not to delete any emails which relate to the area under investigation. They should then be asked to identify and make available any relevant emails for inspection. The compulsory nature of this instruction, the need to ensure comprehensive disclosure and the necessity of its swift completion should all be communicated to the user (who may otherwise consider it to be of low priority). The relative ease with which staff are able to carry out their role in this process will largely be determined by the degree to which the measures outlined in the creation and active use phases of this resource have been adopted.

Final Outcome

As with all other types of information it is important that any emails worthy of long term or even permanent retention are identified and managed in such a way as to enable continued access to them in the years to come. Conversely it is equally important once the decision has been taken to delete an email that all instances of it have been completely and unequivocally removed. This last phase of the lifecycle focuses on these two possible final outcomes.

The contents of this section build on and augment the information provided in the Information Lifecycle - Final outcome strand and should be considered in this light. What this section attempts to do is build on the general good practice guidance on information management covered previously and look specifically at the additional requirements for managing emails.

As such it will be of use to those tasked with managing and maintaining email services within the institution and those with an interest in the management of information and records.

The topics covered within this section include:

- Archiving & preserving emails
- Deleting emails

Archiving & Preserving Emails

It may seem unlikely that your institution will ever want to permanently preserve an email - after all they are hardly the same as the ancient charters written on parchment, or the vast ledgers and accounting books which may feature in your historical archive. But it is important to remember that years ago those ledgers and accounting books were also seen as bland functional, administrative records of operational rather than historical value. The emails informing staff that the institution has been awarded university status or is to merge with another college are obvious examples of messages which need preserving as part of the historical record. Other examples might be less obvious but are likely to be characterised as emails which answer the what, when, why, who and how questions associated with major developments within the institution. As ever, the secret is not to manage emails based on the fact that they are emails, but according to their content. As such emails of potential historical value should be identified and captured according to whatever policies your institution has in place for identifying its archival records. The [guidance on Archival Appraisal](#) which accompanies the JISC infoNet Records Retention Schedule provides advice in this regard.

Alongside the few 'historic' messages which may require permanent preservation there is also likely to exist another category to be considered: those emails which for operational reasons need to be retained and accessible for a long period of time. It is hard to put a precise number of years against what constitutes a 'long period of time', but when talking about information held in electronic format this could be as little as anything older than five to ten years. Without taking special measures to ensure their continued longevity it is likely that emails older than this will lose some or all of the characteristics required to retain their evidential status as records (see the [records management](#) strand of this resource for further details of these characteristics). Emails relating to building projects, long term contracts, research trials and employment matters amongst others could all fall into this category.

The measures required to preserve such emails and to provide continued access to their content can be complex and will require a mixture of policy, technology and user participation - starting with the need to identify potential candidates for preservation at the earliest possible stage. This will inevitably require the participation of users so training and awareness of such issues as part of general email training is likely to feature as an important first step.

The JISC Digital Curation Centre has produced an excellent, detailed, set of guidelines on the [curation of email](#). It is a comprehensive, yet readable, guide to the subject and is recommended as the source of detailed guidance in this area.

Deleting Emails

The process of deleting and destroying email is of course closely associated with the subject of retention - destruction being the logical outcome when an agreed retention period has come to an end. As such the guidance in this section should be read in association with the sections on email retention.

However, rather than focusing on when an email should be scheduled for destruction the purpose of this section is to explore the issues surrounding the actual destruction process.

Has Your Deleted Email Really Gone?

It is important that the process of deleting emails is comprehensive, complete and irrevocable. After all, there is little point in ensuring the destruction of one copy (perhaps the one held in the sender's sent items folder) if each of the five recipients has retained their own copies. Even if the intention is for the email in question to have been removed the fact that a copy still exists is enough for it to be disclosable under FOI or as part of a legal discovery exercise. The need for such a comprehensive approach to email destruction is one reason why the author of this resource favours the introduction of an automated email deletion process after a relatively short period of time - even with its attendant cultural and procedural problems. However even this will not be sufficient if users are routinely storing their emails 'offline' either individually or collectively as monthly .pst folders to escape the automatic deletion process.

As stated above, email deletion must also be irrevocable. The guidance from the [Information Commissioner's Office](#) is explicit in its assertion that:

"Information located in desktop recycle bins is clearly subject to the FOIA as this continues to be held and is easily accessible. Once deleted from the recycle bin the information will also continue to be held unless the electronic record is completely erased from the computer system."

The issue becomes slightly greyer when it comes to the subject of email stored on back-up servers as the following quote from the same source indicates:

Information in a deleted file or in a back-up, whether a server, disc or tape, may be regarded as being held by a public authority for the purposes of the FOIA depending on the particular circumstances of the individual case. (Our position on this issue has been modified in the light of the Information Tribunal decision in [Mr P Harper v The Information Commissioner EA/2005/0001](#)).

For the avoidance of doubt it is therefore recommended that procedures be put in place to ensure that the contents of back-up tapes and servers are also subject to pre-defined, agreed and documented retention controls. This will help prevent both potentially expensive trawling of vast volumes of data potentially stored in multiple locations and the possible disclosure of messages thought long departed.

RECORDS MANAGEMENT

INFOKIT



www.jiscinfonet.ac.uk/infokits/records-management

Records Management

What Is Records Management?

Records management is an established theory and methodology for ensuring the systematic management of all records and the information they contain throughout their lifecycle.

According to International Standard ISO 15489: 2001, records management is defined as:

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

A detailed description of what constitutes a record will be explored further in the section [What is a record?](#). Traditionally records were held on paper, microfilm or microfiche, but are now predominantly created and held in electronic format or within electronic systems.

The core concept underpinning records management theory is that of the lifecycle, which sees records having a series of phases from creation to final disposition ultimately resulting either in their controlled destruction or being retained on a permanent basis as an archival record.

This infoKit is based around the well established concept of lifecycle management and how it should be specifically applied to the management of records. Further information about the general theory underpinning the information lifecycle, the main phases within it and the key concerns and issues to be addressed within each phase is available from the [Managing the Information Lifecycle](#) strand of this resource.

The principle reason for applying the lifecycle concept to records management is to ensure that the records being created and held by the institution are being managed and maintained in such a way that they:

- meet all internal business needs
- enable the defence of the rights and interests of the institution and its stakeholders
- enable the content of the record to be accessed, used and reused in a controlled and efficient manner
- is compliant with all regulatory and statutory requirements
- is capable of providing evidence of a transaction or business process which is admissible in a court of law
- is kept and maintained/stored in the most economical way consistent with the above objectives
- is disposed of in a way which is auditable, and meets all environmental and other requirements

According to International Standard ISO 15489: 2001 records management includes the following activities:

- *setting policies and standards*
- *assigning responsibilities and authorities*
- *establishing and promulgating procedures and guidelines*
- *providing a range of services relating to the management and use of records*
- *designing, implementing and administering specialized systems for managing records and*
- *integrating records management into business systems and processes*

Why Is Records Management Necessary?

All further and higher education institutions are large and complex organisations. They employ hundreds if not thousands of staff, undertake a varied range of functions and have complex administrative structures often straddling multiple geographical locations. In order to operate as modern, agile and efficient organisations able to sustain growth and manage change it is essential that they have effective control over the records they create and use. Historically the way in which internal records have been managed has developed in a piecemeal, organic fashion - often in response to local departmental requirements. It is now increasingly recognised that a more proactive, consistent and comprehensive approach is required for the institution to be able to cope with current and future demands.

All institutions and their staff are under pressure to do more for less. This might be as a direct result of an ever-increasing volume of students, or as universities are encouraged to branch out into new agendas such as business and community engagement. Creating accurate, reliable records; providing controlled, ready access to them and only retaining those worthy of preservation are all part of the essential infra-structure necessary to meet these challenges. This is especially true as it becomes less and less possible to rely on the knowledge and experience of individual members of staff. Increased staff turnover and regular organisational restructuring mean that the records an institution creates now represent its 'collective memory' to a far larger degree than ever before.

Institutions are also becoming increasingly aware of the potential value contained within the internal records they hold. This could be the lessons they contain from past experiences, allowing institutions to learn both from their successes and their failures. Alternatively as knowledge-rich, research-driven organisations it could be the competitive advantage or even commercial gain that can be acquired through the effective exploitation of their information assets.

As the evidence left behind from the activities we undertake, records are also an institution's best ally in terms of protecting its rights and interests. Effective records management ensures that the institution can call upon a body of reliable evidence if required to justify its actions, or defend its position. This may prove a critical strength as we move into an increasingly litigious society.

Institutions are also under ever-mounting pressure to proactively demonstrate their accountability and good standards of corporate governance. This may take the form of internal audit, submissions to funding bodies or public scrutiny through legislation such as the Freedom of Information Act, Environmental Information Regulations and Data Protection Act. Compliance with all of these is only possible if the appropriate body of records exists to prove what actions were taken, why they were taken and on whose authority, and what their outcomes were. This is only possible with effective records management.

Creation

Whilst all records are information, not all information is a record. In this section we will therefore analyse what are the unique properties that separate records from more generic sources of information or data and as a result what is required to produce good, reliable records.

The contents of this section build on and augment the information provided in the Information Lifecycle - Creation strand and should be considered in this light. What this section attempts to do is build on the general good practice guidance on information creation covered previously and look specifically at the additional requirements for creating good **records**.

As such it will be of use to those tasked with managing records within the institution, quality managers, auditors and those responsible for the design of new systems and processes.

The topics covered within this section include:

- What is a record?

- Creating authentic records
- Creating complete records
- Creating reliable records
- Fixity and declaring records

What Is A Record?

The ISO defines **records** as *"information created, received, and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business"*.

Whilst useful in stressing the essential evidential quality of a record and of highlighting the vital role played by the record as the output of a transaction, it could be said that this definition of a record fails to adequately describe the properties which define a record.

The International Council on Archives (ICA) Committee on Electronic Records definition of a **record** as, *"recorded information produced or received in the initiation, conduct or completion of an institutional or individual activity and that comprises content, context and structure sufficient to provide evidence of the activity"*. The [International Council on Archives](#) goes some way to addressing these short-comings by stressing three key properties inherent in all records, that is that they must possess:

1. **Content** (i.e. information or data)
2. **Context** (i.e. it must be possible to ascertain how it relates to other records and to the organisation which created it)
3. **Structure** (i.e. there must be an inherent logic to the way in which the information it contains - and the metadata which is likely to define its context - are laid out and which is ultimately interpretable by the human eye)

The result of adhering to these properties should be to create records which contain the following qualities:

1. **Authenticity**. It should be possible to identify, and preferably prove, the process which created the record and who its authorised creator was.
2. **Completeness**. The record should contain all of the content required to act as evidence of the transaction it is documenting. This does not mean that one record must contain *everything* to which it relates; simply that it is complete in its own terms.
3. **Reliability**. It is important that the content of the record can be relied upon as an accurate representation of the transaction it is documenting.
4. **Fixity**. Once declared as a record its content should no longer be altered or changed in any way. It is in this way that its evidential value is preserved (by ensuring that the content of a record remains exactly as it was at creation).

Finally, it should be noted that all of the above properties and qualities can apply regardless of the record's format, whether it be a sheet of paper, email, photograph or database entry.

Such precise definitions and their theoretical underpinnings may seem complex and largely irrelevant to practitioners at the 'coal face' within institutions. However, as we shall see throughout the remainder of this strand of the infoKit they are relevant and do have a very real and practical application. It is largely this definition of what records are which separates them from other types of information or data, provides them with their added value and, as we shall see, defines the way in which they must be managed.

Creating Authentic Records

The concept of *provenance* is a key aspect of records and archival management theory. It describes proof of the origin or source of something (in this case a record) and the chain of custody regarding whose hands it has passed through since.

Why Is This Important?

Capturing a record's provenance provides proof as to who the actors were in any given transaction or process and demonstrates that they had the appropriate authority to undertake it. It should also provide guarantees regarding the reliability of the content due to the known position and authority of the creator. Controlling and recording the 'chain of custody' then perpetuates these assurances throughout the remainder of its life. This issue is explored in more detail during the [Active Use section](#) of this infoKit.

How To Create Authentic Records

Given the importance of provenance to creating authentic records, it is vital that the institution has clearly defined processes surrounding the transactions⁵ it undertakes. This not only means knowing precisely how the transaction should be conducted, but also who should be involved within it and what their specific roles are. The JISC infoNet infoKit on [process review](#) should help institutions in this regard. As part of this exercise, it is important to identify what records will be created at which points in the process, thus closely associating each record to the process they are documenting.

It is often the case that systems which create structured data, such as relational databases, student record systems etc are better equipped to automatically control and capture record provenance. Access is usually via a password controlled login which validates the identity of the creator. Any records created or edited during that session will then be automatically associated to that particular user. The user's profile can also be used to determine what system rights they have access to and therefore what transactions they can undertake.

It can be more difficult to achieve this level of control with unstructured records such as text-based documents, spreadsheets etc. Measures to address this may include:

- Limiting access to particular areas of the record storage facility (i.e. particular folders or areas of the file plan) to specific identified users
- Creating official templates for use when creating specific record types (meeting minutes, project plans, annual review forms etc) and limiting access to them to certain identified users
- Ensuring the document properties are picking up the correct authors name from their log in and/or making manual completion of the author field mandatory on document creation
- Considering the use of biometric authentication systems to confirm the identity of the creator
- Ensuring the 'header' metadata documenting the transfer information is retained with any emails saved outside of the email client

Creating Complete Records

⁵ It should be noted that when we refer to 'transactions' this does not necessarily mean financial transaction. The term transaction can be used to describe the completion of any process and could equally apply to a holding a meeting, agreeing a project plan, appraising a member of staff or disciplining a student

Creating records which contain all relevant content and contextual information not only ensures that the transaction in question has been fully and appropriately documented, but also that the record has value as a source of information to others.

Why Is This Important?

Any 'record' which has parts of its content missing, or is otherwise incomplete, will clearly not be reliable as a source of evidence and is likely to be disregarded as such. This could leave the institution unable to explain its actions and thus defend its legal interests.

Incomplete records not only reduce their informational value, they can also prove to be positively misleading and potentially dangerous. The user may not be aware of important additional information, amendments or clarifications which may fundamentally alter the meaning of the record. This may lead to well-meaning but incorrect decisions being made based on false assumptions.

Records that are incomplete will be reliant on the memory, knowledge or experience of the end user to 'fill in the blanks'. Where all staff are in possession of such skills, this may not be an issue in the short term. However, temporary contracts and high staff turnover mean that few areas of the institution will be in this situation. Furthermore, the longer after the point of creation that the record is accessed for information, the less likely it is that the memory of staff can be relied upon to 'fill in the gaps' - thus increasing the risk.

How To Create Complete Records

- When designing a new record-creating system, define exactly what information it is appropriate to capture (time/date, location, author, purpose, outcome etc) and where possible use system design to capture this information automatically as part of carrying out the transaction
- When designing document and form templates consider their design and specify which elements must or should be completed. Use document properties to enforce completion of all mandatory elements
- When archiving emails as records ensure that all component parts of the message are retained as a complete set (for example, content of message, transmission information and attachment(s)). Further information on management of emails as records is available from the Email Management strand of this infoKit
- Ensure any files containing OLE links to other associated files are managed consistently and that the links are retained. This may be especially important when moving files from one location within the file plan to another, or when deleting some files.

"OLE: Object Linking and Embedding (OLE) is a technology that allows embedding and linking to documents and other objects, developed by Microsoft. It is founded on the Component Object Model. For developers, it brought OLE custom controls (OCX), a way to develop and use custom user interface elements."⁶

- Consider the appropriate 'unit of management' for a record. For example, when managing web resources, does each webpage stand alone as a complete record, or is it more appropriate to consider the complete website as the record?

Creating Reliable Records

⁶ Taken from the Wikipedia entry for Object Linking and Embedding on 09 July 2007
http://en.wikipedia.org/wiki/Object_Linking_and_Embedding

Alongside authenticity and completeness, reliability is the third key quality common to all records worthy of the name. In many regards a record's overall reliability will, to a large extent, be determined by the degree to which these other two qualities are present but it also exists as an important quality in its own right. A record may have been created by the appropriate, authorised person and it may contain all of the elements that it should but these will count for little if that content is itself factually incorrect.

Why Is This Important?

The institution faces the same risks if creating unreliable records as it does if creating incomplete records, in terms of decisions being made based on inaccurate data. However, where content is present but incorrect that risk is increased. This is because the likelihood of it being accepted as the truth and acted upon as such is correspondingly higher. It is not difficult to imagine examples of where incorrect information stated in unreliable records could materially damage the interests of stakeholders. For example, incorrect grades associated to a student, the wrong salary paid into a member of staff's bank account or measurements mistakenly recorded in feet rather than metres on a plan.

It should also be remembered that when dealing with personal data it is a legal requirement to ensure that records containing personal data are [*accurate and where necessary up to date*](#).

Lastly, as the main source of the historical record charting the development and progress of the institution, it is clearly in its long term interests to ensure that the records it creates are as accurate and reliable as possible.

How To Create Reliable Records

- User training is often overlooked as a critical aspect for ensuring the creation of reliable records. With a few notable exceptions (for example minute taking training for secretaries) there is often little emphasis placed on training staff to accurately record the transactions they perform. IT training is a good example where staff will be trained on the details of how to use Microsoft Word to create a document, but seldom on what it is they should be using it to create.
- System design should reduce the amount of data fields requiring manual entry by relying on macros and formats which enable data exchange between systems (such as XML).
- Errors often occur when staff are pressed for time and attempting to deal with a range of processes at any one time. The institution should attempt to create a culture which acknowledges that time spent creating accurate, reliable records is equally as valuable as that spent performing the functions to which they relate.
- Good practice itself helps create a 'virtuous circle'. If users have access to accurate records when researching their work, the chances of them themselves creating accurate and reliable records is increased.

Fixity & Declaring Records

We now live in an age where we expect information to be fluid. Database content is continually changing, web pages are updated by the minute and our news programmes now come as constant 24 hour rolling broadcasts. Yet from the records management perspective it is vital that at set points in the process we draw a metaphorical line in the sand and fix the content of a record as it stands at that point. Once fixed it is equally important that it stays fixed - preserved as an accurate, unaltered record of the event in question.

Why Is This Important?

The importance of this concept of fixity stems again from the fact that records have an importance and purpose above and beyond simply the information they contain. In order to function as

evidence, it is vital that records are an accurate and contemporary record of how things were at the time of the record's creation. Obvious examples of when this might be important include the terms of a contract agreed with a 3rd party which must stand for the duration of the contract or procedures introduced to govern how research projects must be conducted. Without agreement as to when these key records have reached their final, approved state and subsequent assurances that their content has not been altered it is easy to predict the potential disputes and challenges which may arise.

Things do, of course, change over time and the records we created must reflect that. The concept of [Version Control](#) is covered in the next section of this infoKit. For now we are focusing on the initial point at which the content of the record is fixed, a process commonly known as *declaration*. All records will have a life before they are declared as a record and their contents fixed. They will be drafted, edited and redrafted as draft documents many times before their contents are agreed, finalised and ready for any formal sign-off procedure. It is at this point that the process of *declaration* should occur and a record be created.

How To Declare Records

- However, the act of declaration is achieved the result should be the same. That is that the contents of the record are frozen at this point and should remain un-editable from thereon. Also that any associated metadata is likewise fixed to reflect their state at the point of declaration. Particular attention may need to be paid to ensure dates do not alter (e.g. not updating the date last edited every time the record is subsequently viewed after declaration).
- It is important that the principles of provenance are also considered . For example, that the name of the creating department as stated in the metadata remains as it was at the time the record was created, even if subsequently changed during a re-structuring process.
- Care should be taken to consider the entirety of the record at the point of declaration. For example, ensuring that any OLE embedded files are also declared at the same time, or that external information on which that record is reliant (such as a page on the intranet) is also captured.
- For reasons relating to version control (which will be discussed in full later on -) it is useful to amend file names or other unique identifier codes to reflect the declared status of the record.
- Once declared it should still provide the user with the ability to create a new record based on that declared which will then be treated as a separate entity.

Active Use

The life of a record begins at the moment of its declaration . This means it is already information of some maturity by the time it enters its active use. For records then the active use phase may be characterised less by constant use and rapid change than for other, more informal types of information. Instead the emphasis remains on ensuring the maintenance of the specific qualities and properties of the record which give it its value throughout this first stage of its use.

All of the guidance contained in the general Information Lifecycle Management strand of this infoKit for the active use phase remains relevant and the contents of this section is intended to build upon this work. What follows relates specifically to the management of **records** during the active use phase and should be read and considered in addition to this earlier guidance.

As such it will be of use to those tasked with managing records within the institution, quality managers, auditors and those responsible for the design of new systems and processes.

The topics covered within this section include:

- Managing version control

- Retaining the audit trail
- Managing the master copy
- Protecting vital records

Managing Version Control

Even once declared as a record it is still inevitable that updates will need to be made to a record over time. As we have seen in the previous section, thanks to the need to preserve the virtues of fixity and authenticity, changes should not be made to the content of the original record once it has been declared. Any further amendments, alterations or even corrections should be made and saved as a new version of the record - keeping the original as it was at the time of declaration. In this scenario it is now essential that we retain control over new versions of the record and are able to distinguish when subsequent drafts do themselves become newly declared records.

Why Is This Important?

The same requirement to be able to distinguish between draft documents and final records applies with regards to subsequent versions as discussed in the previous section with reference to their original creation and declaration.

When a record is being updated it is likely that the changes will be made over several sessions, perhaps involving multiple members of staff. Without clear co-ordination of this process and management of the various versions created chaos will soon reign with no clear picture of which is the most current version, and which should be declared as the next version of the record. This risks decisions being made according to out of date information which is believed to be current. It can also lead to potential embarrassment with content which was removed from a previous draft being mistakenly included within the final declared record.

Finally of course it leads to wasted time and considerable frustration both on the part of the author who spends time needlessly working on an old version and the reader who has read an obsolete document.

How To Maintain Version Control

- Agree and abide by a file naming and numbering schema which clearly separates and denotes both draft and final versions
- Ensure only one definitive copy of each record exists to prevent multiple, 'parallel' versions being created
- Include version information as part of standard document design
- Provide reference links to records stored in central shared locations, rather than attaching copies as email attachments
- Consider whether or not to retain drafts once a new version of a record has been created (see the next section - Retaining the audit trail - for further details)

Further details of all of the above are available from the [Managing Information to Make Life Easier: A Practical Guide for Administrators](#).

Retaining The Audit Trail

As we have seen, records represent our best, and often our only, link with the past - whether that be to satisfy our historical curiosity or to prove the legitimacy of our actions. Knowing what a record said at a particular point in time and being able to demonstrate how its content has evolved is key to preserving this link between the record and the process or event it describes.

Why Is This Important?

As well as acting as evidence of the transactions we undertake, many records actually define the boundaries within which these transactions must occur and dictate the way in which they are carried out. For example, the procurement policy which determines how a service or product must be acquired or the research ethics guidelines which provide the guiding principles to which a project must abide. Important decisions are taken against the contents of these records as they exist at the time. It is therefore vital that it is possible to pin-point exactly what the record said at any given point in time in order to re-create these conditions and verify the validity of the decisions made.

It may also prove necessary to be able to demonstrate exactly who made what changes and when. This could be in order to provide proof of who was involved in a process and evidence of their authority to do so or simply to enable the author of a particular version of a record to be identified and contacted to provide clarification over a point of detail.

The audit trail can also help show how ideas developed over time and in response to specific events. All of which can be valuable from a 'lessons learnt' perspective.

How To Retain The Audit Trail

- It is impossible to be able to maintain and recreate a record's audit trail without effective version control using some or all of the measures outlined in the previous section.
- Careful thought should be given as to whether it is appropriate to retain previous drafts of a record once the final version has been declared. Doing so will obviously provide a fuller history of the development of the record which may be useful. However, it will also add significantly to the overall volume of information being held by the institution and may increase the risk of inaccurate information being inadvertently retained and brought back into circulation. Once declared as a record it should only be deleted in accordance with your retention management policy, even if superseded by more recent versions.
- Ensure you consider the most appropriate format for maintaining records. Some media may be excellent for allowing easy drafting and editing of content but this transience can make it difficult or impossible to accurately 'roll back' the content to a specific date or version.
- If you are going to use your website or intranet to store and publish the only copy of records such as your prospectus or operating procedures, ensure your content management system does retain a full date-stamped audit trail of changes made. Alternatively, you may need to introduce manual measures such as ensuring that a separate 'snap-shot' of the content is taken and preserved as the formal record of the content at any given time.

Managing The Master Copy

Thanks to the ease with which new records can be created, copied and circulated, it is inevitable that multiple copies of records will still exist - even if the creation and version control advice featured in previous sections is followed. For example, all members of a committee each receiving their own copies of the minutes and associated papers.

It is necessary to strike a balance between the need to extend appropriate management controls to all information held by the institution (as outlined in the [Managing the Information Lifecycle](#) strand of this infoKit and the separate need to identify and manage the master copy of a record as a prime concern.

Why Is This Important?

It may be that the master copy of a record has additional unique properties which give it added value and significance over any other copies which may exist, for example if it contains an official signature.

Alternatively, it may be that different management requirements exist for the master copy than for associated copies. For example, a record requiring long term preservation may need to be migrated to a more stable open format. This is an exercise you only wish to perform once on the definitive master copy and not repeat unnecessarily on further copies.

Lastly, as we shall explore in more detail in the section on retention management the master copy will usually have different retention requirements than will apply to other associated copies.

How To Manage The Master Copy

- Identify the agreed source of the master copy (for example the copy of the minutes signed by the committee chair, or the project sponsor's version of the Project Plan.
- Consider establishing procedures for ensuring the capture of master copy at the point defined as the end of its active use (end of project, year end etc). This will be linked to the steps outlined in the Information Lifecycle Management - semi-active use - Do you know [what information is being held and why?](#) Section.
- Issue an umbrella policy statement regarding whether the institution considers the paper or electronic version of records to be the master copy (where appropriate). This will need to consider the institution's ability to preserve digital records in the long term, plus the legal position regarding the use of electronic information as evidence.

Protecting Vital Records

Vital records can be defined as those categories of record which are required by the organisation to be able to carry out its essential core functions in a legally compliant manner. As such they make take many forms ranging from historic charters, through to estate records, insurance certificates, staff payroll information and emergency out-of-hours contact details for key staff.

Why Is This Important?

The quickest way to describe the importance of such records is to imagine the situation without them. The institution may have no legal mandate to provide education, may not be able to prove ownership of its built estate nor allow those few staff who are willing to work without payment to operate without appropriate insurance cover.

This may represent the most extreme, apocalyptic vision but even the 'milder' consequences resulting from the loss of vital records are certainly to be avoided at all costs. These include loss of intellectual assets and competitive advantage, inability to protect the interests of stakeholders (for example, providing proof of qualifications gained by former students) and of course severe damage to your reputation.

How To Protect Vital Records

- Clearly the first requirement is to be able to identify and locate those records which are deemed to qualify as vital. This process may prove easier if broad categories of types of vital record are first defined. Some example categories are included in Table 1. Identification of the master copy as outlined in the previous section will assist in this process.
- Additional management controls will be required for vital records. These are likely to include routine duplication together with off-site storage of back-ups, specific finding aids

which allow vital records to be found quickly and easily in the event of a disaster and ensuring that management of vital records is co-ordinated with other aspects of the institution's disaster recovery and business continuity planning measures.

- Measures put in place to manage vital records will need to cover both existing records, plus all new vital records created in the future. The information audit process described in a later section will prove invaluable for locating existing vital records. When it comes to preparing for future records it will prove useful to identify the processes which will create the records in question.

Table below - Example categories of vital records plus examples

Legal	Charters, insurance certificates, deeds etc
Financial	Accounts, payroll, pensions etc
Operational	Timetables, exam papers, student records
Commercial	Contracts, memoranda of understanding etc
Intellectual capital	Research data
Disaster recovery	Out of hours staff contact details, estate plans, utility and emergency service contact details

Semi-Active Use

As with all categories of information, the semi-active use phase of the lifecycle is often the most difficult to define and control when it comes to the management of records. This is particularly true for records as the longevity of their *evidential* value often far exceeds that of their *informational* value. As a consequence a significant volume of records often need to be retained which appear to the casual observer to be of little relevance or importance. The ability to separate the 'wheat' from the 'chaff' and manage them accordingly during this phase may play a pivotal role in protecting your institution's long term interests.

All of the guidance contained in the general Information Lifecycle Management strand of this infokit for the semi-active use phase remains relevant and the contents of this section is intended to build upon this work. What follows relates specifically to the management of **records** during the semi-active use phase and should be read and considered in addition to this earlier guidance.

As such it will be of use to those tasked with managing records within the institution, quality managers, auditors and those responsible for the design of new systems and processes.

The topics covered within this section include:

- Undertaking a record survey
- Retaining the audit trail
- Retention management

- Records appraisal

Undertaking A Record Survey

Undertaking a comprehensive audit of the records you hold, the processes which create them and the measures taken to manage them represents a significant task. However, its findings are a crucial weapon in helping you manage records throughout their semi-active use and through to their final state.

Why Is This Important?

The records survey provides an objective assessment of an institution's record-keeping practices, and the way in which that information is actually used. In many respects it is the first and most important step towards getting control of records and the information which they contain. It is a time-consuming and labour-intensive process, but is likely to produce insights into many other aspects of the way in which your organisation functions, in addition to its records management focus. For example:

- highlighting where there is unnecessary duplication of records
- indicating where business processes might be streamlined for more efficient administration
- demonstrating where records are being kept too long
- highlighting areas where user training and awareness of records management tasks needs to be increased
- identifying vital records
- uncovering where cost savings might be made through economies of scale etc
- determining preservation requirements

This is not a comprehensive list of objectives, merely an indication of the potential range of knowledge that can be obtained through such a survey and the benefits it may bring.

How To Undertake An Information Audit

Because of scale and complexity of undertaking a full record survey, a separate mini-guide to this process is included within this infoKit .

[Click for the Record Survey Guide](#)

Retention Management

A retention schedule is a list of records for which pre-determined destruction dates have been established. One of the principle aims of the records survey is to establish those categories of records for which there is a known disposal date.

The main objective of the retention schedule is to define how long records need to be retained in order to satisfy all operational, legal and regulatory purposes and to help co-ordinate their resulting maintenance, disposal or preservation.

Why Is This Important?

There is a careful balance which needs to be struck with regards to the retention of records. As we have covered in previous sections, it is important that records are kept for as long as their contents have operational value and for as long as they may be required as evidence of the transactions they document. However, there are often also compelling reasons not to retain such records for any longer than they are required relating to costs of storage, pressures on physical

space and the need to disclose all relevant information you hold in response to an FOI request or legal discovery exercise. When it comes to records containing personal data there are also legal requirements under Principle 5 of the [Data Protection Act](#) which require institutions to not retain personal data for longer than is necessary for the purpose(s) for which it was obtained.

There are also legal requirements governing how institutions and other public bodies should remove the records they wish to legitimately dispose of. According to the [s.46 Code of Practice](#) on the management of records which accompanies the Freedom of Information Act:

"Each authority should maintain a selection policy which states in broad terms the functions from which records are likely to be selected for permanent preservation and the periods for which other records should be retained".

A records retention schedule represents just such a selection policy.

How To Manage Retention

- Consider adopting and tailoring as required either the JISC infoNet HE and FE retention schedule .
- Ensure your retention schedule covers records held in all formats.
- Consider retention functionality when selecting or designing IT systems which will create or store records.
- Consider how retention issues will be handled if choosing to digitise large volumes of records.
- Ensure your retention management not only takes into consideration retention requirements based on the record's content, but also considers the specific format and media electronic records may be stored in.

Final Outcome

This final phase in the records lifecycle leads to two logical outcomes: either the record is destroyed, or it is retained as a permanent, archival record. The main objectives of this phase is to ensure that each record follows the correct path and that the decisions which decide this are made according to pre-determined rules and criteria. For those records which are retained, so new records may in turn be created which draws upon their content or the learning contained within them - thus perpetuating the lifecycle.

All of the guidance contained in the general Information Lifecycle Management strand of this infokit for the *final outcome* phase remains relevant and the contents of this section are intended to build upon this work. What follows relates specifically to the management of *records* during the *final outcome* phase and should be read and considered in addition to this earlier guidance.

As such it will be of use to those tasked with managing records within the institution, quality managers, auditors, archivists and those responsible for the design of new systems and processes.

The topics covered within this section include:

- Record appraisal & disposal
- Preservation & curation

Record Appraisal & Disposal

The act of disposing of a record is not one which should be carried out in an ad hoc or unmanaged manner, but according to pre-defined criteria and clearly articulated processes. This

will ensure that you can justify why the records in question were destroyed, as well as proving beyond refute that no trace of them remains.

Why is this important?

Even if carried out with completely innocent motives, the uncontrolled destruction of records without proper authorisation or due process can easily be interpreted as an attempt to avoid releasing damaging information and prevent the cause of justice. Notorious cases of deliberate unauthorised destruction of records such as at Enron have increased the need to be seen to exercise suitable control over this aspect of records management. The introduction of the Freedom of Information Act in the UK has also increased the importance associated with the need for transparency and accountability during the disposal process and the requirement for an institution to be able to defend its actions if challenged.

Finally, if carried out according to a clear and defined process, the chances of either valuable records being destroyed in error, or the wrong records retained, should be significantly reduced.

How to appraise & destroy records

- Have your records retention schedule officially approved by senior management, thus providing high-level authorisation for the activities carried out according to its content.
- Although your retention schedule will provide the basis for your selection and decision-making process, also be aware that the schedule only defines *minimum* retention periods. Be prepared to consider any special circumstances which may alter the situation for individual records (for example, any record which is the subject of an ongoing FOI request should not be destroyed, even if due for destruction according to the retention schedule).
- Turn the appraisal and destruction process into regularly scheduled business processes, rather than ad hoc events. Establishing a department-by-department timetable can help embed this into the institutional calendar. Likewise, specially organised 'black bag days' can be successful in ensuring scheduled retention actions are actually carried out within offices.
- Ensure *all* copies of records scheduled for destruction are destroyed (including those stored off-site, or electronic records stored on back-up tapes or servers).
- Ensure records are destroyed in a confidential and non-recoverable manner (i.e. incinerated or cross-shredded).
- Consider the level of approval required to destroy records and ensure a documentary audit trail is in place which records the process from selection through to confirmation of destruction.

Permanent Preservation & Curation

Both archival management and digital preservation are vast subjects in their own right. As a result, this section can be no more than a signpost to some of the main issues as viewed solely from the perspective of their implications for records management. In this light the primary challenges faced here chiefly relate to ensuring the ongoing security and safety of permanent records and guaranteeing continued access to them in perpetuity.

Why is this important?

Both the content and evidential value associated with some records may require them to be retained for such long periods of time that as far as any member of staff managing them today is concerned and for all practical purposes they can be assumed to require permanent preservation. For example, some records relating to radiation accidents need to be kept for 50 years, whilst some pension records are required for 75 years after the member of staff has left the institution.

The legal rights and interests of the institution and its stakeholders could be put at risk if such records are not preserved.

As well as the operational or legal value inherent in records, a small percentage will also have enduring historic value as archival records. Such records chart the history and development of the institution and act as its collective memory. They represent an important aspect of an institution's identity and heritage, as well as a potentially valuable marketing tool.

Without appropriate storage conditions physical archives are at risk of decay caused by environmental conditions, (damp, temperature fluctuations, insect infestation etc) and loss due to poor security or a lack of awareness of their intrinsic value.

These same risks apply for electronic records, but within vastly reduced timeframes and as only one of a number of considerable threats faced. The physical media on which electronic records are stored are often extremely sensitive to exposure to damaging environmental conditions and the consequences are likely to be immediate and total. Electronic records are also at risk of being irretrievable due to hardware obsolescence (for example, the decline of floppy disk drives) and the speed of software advances which may leave records created in one version inaccessible, or altered by their replacement.

How to preserve records

- Where possible allocate separate, fit for purpose physical storage facilities with adequate security and acceptable levels of stability in both temperature and humidity fluctuations (Note: cellars, basements and attics - the 'traditional' home of the archive are seldom suitable). See the [National Archives - Environmental Management](#).
- Monitor temperature and humidity levels and take preventative measures if they fluctuate outside acceptable ranges (i.e. install de-humidifiers, heaters etc).
- Ensure you create appropriate finding aids for archival records, which also include details of where the records have come from (their provenance) as well as what they are and where they can be found.
- Arrange and describe archival records according to established principles of archival description (i.e. by preserving their original order, describing them in a hierarchical order, and keeping a record of the administrative history of the department or unit which created them). See the [General International Standard Archival Description, Second edition](#).
- Conduct tests prior to migrating records to a new software version. Does the move to a new version introduce any changes to the content, structure or metadata of the record (e.g. changes to formatting, lost header or footer information etc)? If so you must consider whether such changes are acceptable, or whether they could invalidate the records evidential status and take measures accordingly.

Disclaimer

We aim to provide accurate and current information on this website. However, we accept no liability for errors or omissions, or for loss or damage arising from using this information.

The statements made and views expressed in publications are those of the authors and do not represent in any way the views of the Service.

The JISC infoNet Service offers general guidance only on issues relevant to the planning and implementation of information systems. Such guidance does not constitute definitive or legal advice and should not be regarded as a substitute therefor. The JISC infoNet Service does not accept any liability for any loss suffered by persons who consult the Service whether or not such loss is suffered directly or indirectly as a result of reliance placed on guidance given by the Service.

The reader is reminded that changes may have taken place since issue, particularly in rapidly changing areas such as internet addressing, and consequently URLs and email addresses should be used with caution. We are not responsible for the content of other websites linked to this site.

This material is licensed under the [Creative Commons License](#) - 2007