
Records Management

Overview and Introduction

- What is a Record?
- What is Records Management?
- What is the Lifecycle of Information?
- What are Retention Periods?
- Why is Records Management Necessary Now?
- Legal and Regulatory Compliance
- Adopting a Records Management Programme
- Steps Towards Good Records Management

The Information Audit

- Why Do It and Where To Start?
- Objectives of the Information Audit
- A Health Warning
- The Relationship between Policy and Audit
- A Communication Strategy
- Information Gathering
- Electronic Records
- Good Housekeeping and Making Better Use of Investment

Functional Analysis

- Advantages and Disadvantages of Functional Classification
- A Practical Example

Records Retention Schedules

- Risk Assessment and Vital Records
- Disaster Recovery and Controlled Destruction

Implementation and Review

To Conclude

Sources of Further Information and Training



Records Management

Introduction

Welcome to the Records Management infoKit. This infoKit is aimed at people in Further and Higher Education (FE and HE) who are new to the discipline. It is not a comprehensive guide to becoming a professional records manager but it does provide some guidelines to the issues you will face and some of the techniques for overcoming these. The infoKit provides a framework based on a simplified version of the Australian National Archives DIRKS programme for managing business information. If you come from a library, information or archives background some of the elements will be very familiar.

If you are a professional records manager in a large institution the basic reference material may add little to your knowledge although we will be updating the reference material at regular intervals. Your needs are better met by joining one of the JISC list-serves, keeping an eye on records management matters on the main JISC website, and participating in existing practitioner groups in FE and HE and the Records Management Society of the UK. You may however find the infoKit material useful in raising awareness about records management issues amongst non-specialists in your institution.

Even if you are new to all of this you will find a ready welcome in each of the above. Records Management is a relatively new formal discipline. Practitioners come from a range of different backgrounds, are well aware of the size of the mountain a newcomer may face working on their own, and are good at sharing help and advice informally. You can find help on specifically legal matters from the JISC Legal Information Service, and general advice on records management from ourselves at JISC infoNet. Both of these services are available freely to all FE and HE institutions throughout the UK.

Records management is a wide-ranging management discipline. The necessary skills include ensuring that your institution is compliant in a very practical way with all the legislation and regulation that affects its operations, staff and students. Other elements range from the development of 'good housekeeping' of information and records to long-term preservation (10 years+) of electronic data, and the selection of records for eventual inclusion in the historical archive of your institution.

As records manager you are in an interesting situation in your institution. This could be characterised as 'pig in the middle'. With organisational change being the norm, as records manager you may rapidly become the one person who has an overall appreciation of how your institution actually works and therefore a valued source of practical advice to all. Above all your success will depend on persuading both:

- senior management in your institution that the job is worth doing well
- Your colleagues, for whom records are a secondary matter to their prime purpose of teaching and administration that there are positive benefits to their working situation of 'getting it right'.



Records Management policy and operations, which form the core of this infoKit, are discussed in later sections. Ideally these should sit within an overall institutional Information Strategy framework and be closely aligned to its other elements such as IT Policy and development. In practice many educational institutions in the UK have not developed such a strategy. Even where they have, the ability of the newly-appointed records manager to directly influence it will be limited until they have a recognised and positive 'track record'. This infoKit details technical aspects of the role but also emphasises that much of your time will be spent on communication, negotiation and persuasion. This is not a role for the terminally reticent – if after reading this you find that you need more training or would like to proceed to a formal qualification you will find the possibilities detailed in the final section.

To sum up, Records Management is intrinsically unglamorous but vital to the efficient running of your institution's daily operations. It is also the essential tool which underpins your institution's legal and regulatory compliance.

The Freedom of Information Act, 2000 and The Freedom of Information (Scotland) Act 2002, along with the revision of the Data Protection Act 1998 and the new Environmental Information Regulations all came into full force on 1 January 2005. These are just the latest and most stringent demands being made on record keeping practices in FE and HE institutions in the UK. The link between records management and this legislation is now explicit. Both FOI Acts contain Codes of Practice which although not mandatory will become the standards by which all public sector record keeping practices will be judged. These are –

- for the UK: <http://www.lcd.gov.uk/foi/codemanrec.htm>
- and for Scotland: <http://www.scotland.gov.uk/Topics/Government/FOI/18022/11334>

JISC have produced guidance on all these matters which may be found at <http://www.jisc.ac.uk/publications> and <http://www.jisclegal.ac.uk>.

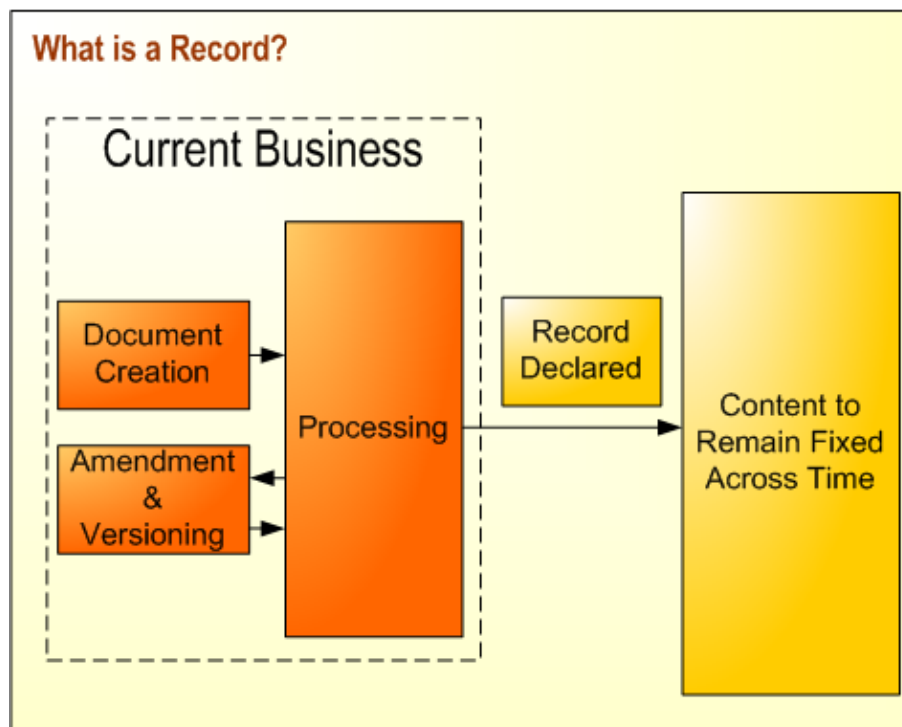
Under your guidance your institution will need to develop record creation and information management policies which are carried through thoroughly and consistently. The basic concept is that information which is captured as a record on paper, microform or in an electronic system requires consistent, systematic and active management from the time it is created until it is disposed of, either by a controlled destruction process or to an historical archive. This process is usually known as the record or information lifecycle.

What is a Record?

Records are the outputs that record each and every business and administrative transaction of an institution and details about its students, members of staff and all its external contacts. They are the essential resource for its effective continuation. They also form its collective memory that must be available beyond the memory or working life of any single member of staff.

The record is the final statement about the transaction or business process which it represents. Once 'declared', it must remain unaltered across time, no matter how many times it is recalled for use. It will contain unique information and/or data and is likely to be the end result of a document and version management process. If the information or data it contains is required for further processing then this should be copied and a new document created.

You must bear in mind that even when the transmission method of a record may use paper and surface mail the document is likely to have been created electronically in a PC using a word-processing package. The original may therefore be the final electronic, pre-printing-out version rather than a photocopy or second printout copy that is placed in a manual filing system. If the paper version is signed or otherwise formally authenticated then that will be considered as the 'original' in law.



What is a Document?

The best way to think about a document is that it is a work in progress by an individual or group of individuals. Only in its final form has it the possibility of becoming a record. All documents and records contain information and/or data and require tags or metadata so that they can be identified and retrieved. Formal document management systems are widely used, to control and track development through versions and editing, but at some point a final version is decided upon, and it is this version that has the possibility of becoming the record.

From what has been said already not all documents become records, and similarly not all records are documents. A record can also take the form of a database or its elements, film, sound recording, and a number of other possibilities.

What is Records Management?

Records management is a process for the systematic management of all records and the information or data that they contain. Traditionally these were held on paper, or more recently on microfilm or fiche, but are now held increasingly within electronic systems.

The core concept is the life cycle of information, which sees information having a series of phases from creation to final disposition either through a controlled destruction process or being added to the long-term or permanent record (the archive) of the institution or organisation it represents.

In most cases that lifespan can be pre-determined at the creation of the record by use of pre-defined retention or destruction schedules.

Good Records management is based on the principles of regular review and controlled retention or destruction of information

The aim is that a record must be managed and maintained in such a way that it;

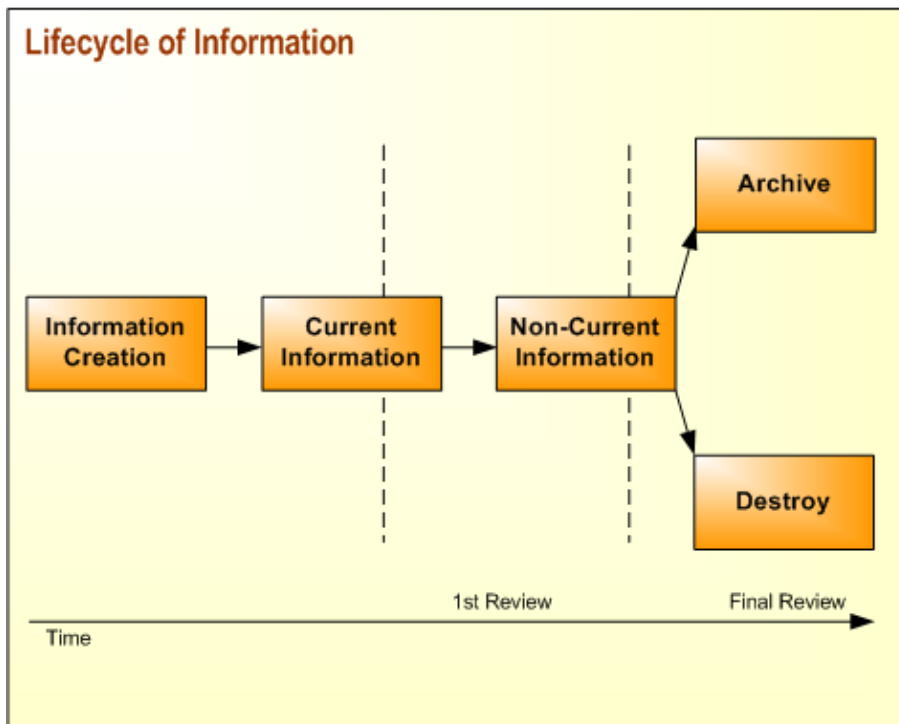
- Meets all internal business needs
- Defends the Institution and its people against all external demands
- Is compliant with all regulatory and statutory requirements
- Is capable of providing the primary or secondary evidence of a transaction or business process which is admissible in a court of law
- Is kept and maintained/stored in the most economical way consistent with the above objectives

And finally

- Is disposed of in a way which is auditable, and meets all environmental and other requirements.

What is the Lifecycle of Information?

Traditionally the lifecycle has been represented by a linear diagram with the horizontal axis representing 'time' from creation.



The review process can be simplified by assigning pre-defined retention periods to categories of information at the information creation phase.

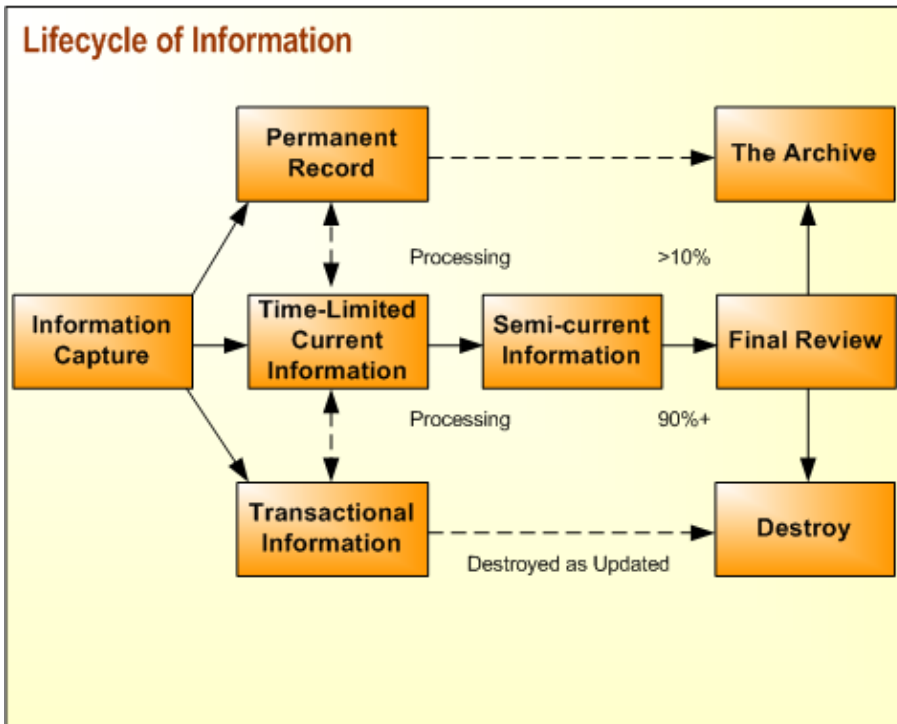
If we ask the question, 'How long should any record remain a current record, likely to be needed for daily business?' the answer is not straightforward. **Time** from creation of the information in the record can never be the sole criterion. Common sense would suggest that different business functions need to keep a record close to hand, that is current, for different periods of time. In some cases it could be as little as a few days, in others it could be several years.

For example, the length of time a student record remains active will depend

- upon the length of the course
- whether the student progresses to another course at the same institution
- whether it is a course leading to a recognised profession qualification. Areas such as medicine, nursing, architecture, engineering, law may require that some elements of the student file are retained for at least the working life of the individual.
- whether the institution uses an electronic student information system which is set to retain student data 'for ever'

Similarly, the semi-current phase will last for varying periods of time. It is best defined as the period of time in which the record might be needed but not regularly.

In practice information flows through an institution are more varied and have differing requirements. It is useful to represent these as three information flows representing different requirements on the information.



This represents a more dynamic view of the life-cycle process. **Time** from creation becomes less crucial than the **function** which the information records.

The **Permanent** Record will include categories such as minutes of governing bodies, articles of association, audited annual accounts, examples of published material, and many others. The key criteria for inclusion in this category are that it:

- will be required for as long as the institution has an existence
- is a permanent legal requirement, or alternatively
- becomes part of the historical archive

Nowadays **Transactional Information** is almost always contained within electronic systems and is information that has no beginning, middle or end state although there is likely to be an audit trail of changes. In most processes it represents a first stage of data processing and is likely to be represented as processed information in the time-limited information flow. This may in turn be further processed and summarised as part of a permanent record.

One example is the progress of the information in a purchase invoice through to a final audited and published account.

The **Time-limited** information stream has two phases. At first it is current information which may be used on a daily or weekly basis. The second phase is when the information has to be maintained for legal or other reasons, but is rarely required for operational purposes. This is the information flow to which **retention periods** can be applied.

An example here is the student record which will be required on a regular basis while the student is attending the institution and their progress is being monitored on a regular basis. This is current information. After the student has left the information will become non-current but parts of that record will be maintained for many years and may be required on a very occasional basis.

What are Retention Periods?

These are the periods of time, varying from a few months to permanency during which a record has to be maintained by an institution. This is usually determined by statute, legal, regulatory or business compliance, or where these do not apply, by a best assessment of risks involved in destruction against the costs of retention. The retention period may consist of:

- ***A fixed number of years from creation:***

Most financial records of organisations have to be kept for the current year +6 years to meet VAT and Tax regulations, an effective total of 7 years. In this case the destruction date is known, fixed and can proceed without further intervention.

- ***The life of the transaction + a fixed period of years.***

Commercial contracts must be maintained for the life of the contract + 6 years. The exact number of years will depend upon the period of the contract.

In some cases records created on the same day for the same type of transaction and apparently similar may be due for final destruction years apart. Student records again provide an obvious example. Detailed records of nursing students will be required for the whole working life of the nurse. It does not follow that every piece of paper or information which is included in such a 'file' has to be maintained throughout. Legislation (Data protection) common sense and efficiency dictate that the 'file' content should be reviewed, and the minimum necessary kept. Pension, student and many types of Human Resource records fall within this category. In many organisations the practice is to review such files after 5 years, review the content, remove all superfluous material and in effect create a new file, or files, some of which may be individually organized according to disposal date. This process will be recorded and audited.

A suggested list of retention periods for further and higher education institutions may be found as part of the [JISC Study of the Records Lifecycle](#).

Recognised Standards

The Codes of Practice noted in the introduction to this infoKit are based on internationally recognised standards of practice for records management in the English-speaking world. While these tend to be very detailed and are prescriptive in tone it is certainly a good idea to have these on your bookshelf for ready reference. No-one would recommend that you know these by heart, and they are not bedtime reading. On the other hand they are clear and objective standards by which your work can be judged both by your peers and by outsiders, and most have summaries of the key points, which are very useful in the persuasion process.

These standards fall into three categories:

- Technical standards for information security, records management, microfilm and electronic records management
- How to provide records which are capable of being recognised as authentic in a court of law
- Certification of copy documents

The purpose of these standards is to provide a guarantee of the authenticity and integrity of a copy of any record being produced for **any** purpose. Why is this necessary?

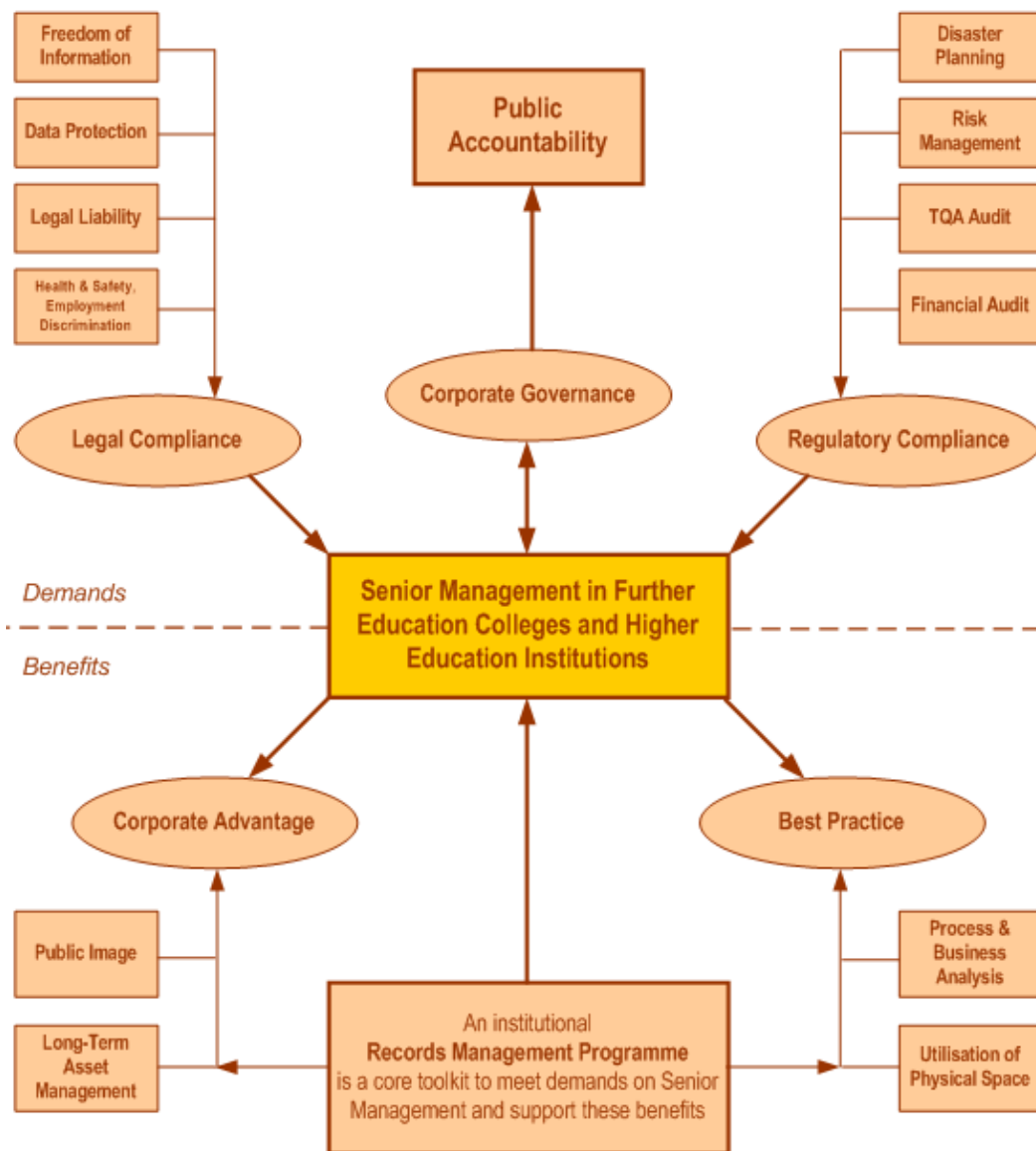
There is increasing anecdotal evidence that the authorities are drawing a distinction between records management and information processing, that is to say situations in which the record could or could not be altered before it is submitted. The distinction is particularly important in the case of electronic records.

To view these in greater detail [click here](#)

Why is Records Management necessary now?

- All further and higher education institutions operate in a complex legal and regulatory world. The penalties for non-compliance are increasingly harsh, both personally for the individual member of staff, and for the institution.
- We live in an increasingly litigious society, that believes it should be rewarded, or at least compensated, for others' failures.
- The natural instinct of most institutions given this scenario is to close ranks and release the minimum information possible to the public. This is not an option anywhere the UK Public Sector. Closer public scrutiny and audit of every aspect of an FE or HE institution's organisation and outputs is demanded in the name of good corporate governance.
- The Freedom of Information (FOI) Acts came into full force in January 2005. All written enquiries and emails have to be answered within 20 working days. To complicate life further Data Protection enquiries have to be answered within 40 Calendar days and Environmental Information requests within 30 Calendar days. If these requests are for information under FOI they can come into any member of staff, and do not need to say why the information is wanted.
- The personal memory of individual members of staff about past initiatives, procedures and organisation is becoming less reliable
 - ◆ as staff turnover increases;
 - ◆ as institutions grow rapidly and change their organisational structure more frequently.
- Records management is a key driver in increasing organisational efficiency

The choice is between muddling through and hoping all will be well, or instituting a records management programme.



Legal Compliance

Legal Compliance is the main driver. The most important statutory areas are;

- Freedom of Information Acts (2000 and 2002)
- Data Protection (1998)
- Health and Safety
- Employment Law
- Human Rights (2000)
- Animal Welfare Acts And Regulation
- Contractual Relationships
- Environmental Information regulations

The JISC Study of the Records Lifecycle quotes 13 separate Acts of the UK Parliament, and over 30 Statutory Instruments of the UK Parliament in compiling its list of recommended retention periods for records of UK FE and HE institutions. To this must be added all statutes which do not give specific guidance on records retention but operate from a series of general principles.

The most important of these are:

The Freedom of Information Act 2000 and the Freedom of Information (Scotland) Act 2002

These two acts, which are in most respects similar give every member of the public the right of access to information held by every public authority in the UK, subject to a number of specific and limited exceptions. They are the direct result of the government commitment to transparency and open government. The Acts have two requirements:

- That all public authorities maintain a publication scheme which is approved by the Information Commissioner, and details the information which the authorities will publish as a matter of course.
- After 1 January 2005 anyone may request information from a Public Authority, has the right to know whether or not the information is held by the authority and normally will have the right to have access to it.

A full text may be found at [Freedom of Information Act 2000](#)

A briefing note by JISC can be found at [Freedom of Information Act 2000 : implementation & practice](#)

A full text of the Scottish Act may be found at [Freedom of Information \(Scotland\) Act 2002](#)

A briefing note by JISC can be found at [Freedom of Information \(Scotland\) Act 2002 : implementation and practice](#)

Data Protection Act 1998

The [Data Protection Act 1998](#) is primarily concerned with protecting the rights of individuals to their personal data. It also defines eight principles with which those controlling or processing data must comply Personal Data must be:

- Processed lawfully and fairly
- Obtained only for a specified purpose or purposes
- Adequate, relevant, and not excessive for the specified purpose
- Accurate and up to date
- Only kept as long as is necessary
- Processed with due consideration for the data subject's rights
- Kept securely
- Not transferred outside the European economic area

One reason why records management is vital to Data Protection is that since 1984 when the first act was passed the definition of what is to be included as personal data has been steadily enlarged. At first it applied only to data in computerised systems. The 1998 Act extended this to all personal data in 'structured' files. On 1 January 2005 this was extended to unstructured personal data as well.

Regulatory Compliance

Regulatory compliance is almost as important as legislative compliance. This is an important element in both good management and institutional efficiency. Elements include:

- Funding
- Teaching Quality Assessment
- Research Quality
- Financial Audit

- Risk Management
- Disaster Planning and Business Recovery

Benefits of Adopting a Records Management Programme

The key question which you will always be asked is 'What is this going to cost?'

That is a difficult question to answer definitively because in part it will depend upon the size of the institution, the results of the information audit (discussed later), the length of time that is available to achieve results, and the amount of human resource available for the task.

The honest and short answer is that there will always be upfront costs but the aim is that these will reduce both revenue and capital expenditure over a 3–5 year period and produce on–going business efficiencies. Exactly how you go about calculating this will depend upon the accounting systems in your institution. The specific matters about which you need information from your finance, property and/or HR department are:

- How property costs are calculated. What you are after is the serviced cost per square metre of floor area in buildings occupied by your institution. This will vary enormously depending upon where you are located, major City centre or countryside. It is entirely possible that the information will not be available in this form and that you will have to make a rough estimate from the information which you can get.
- How depreciation of equipment is calculated. A PC may be considered to be worth nothing after 4 years whereas shelving or furniture may only be written off after 15 years. The potential problem here is that your institution may not have made such calculations, or even have a full scale equipment and furniture inventory. Again you will have to make an estimate based on such information as you can get.
- The average cost per hour of staff at various grading levels. If you are going to attempt to calculate the value of staff time saved by increased efficiency you need to know what it costs in the first place.

Some facts which you might like to take as your starting point.

- An information audit usually produces at least a 50% saving in office filing requirement and even more in storage areas. This benefit can be calculated in terms of the cost of the floor area saved which could be better used for other purposes. It is also a benefit to add the cost of equipment released for other purposes or equipment purchases saved. This is a one–off benefit that can be used to help off–set the initial costs.
- If your institution is moving to new premises or a department is moving to a new building it is rare to have as much storage space as in old buildings. This is usually seen as an opportunity for a clear out. At a practical level what often happens is that the non–current records are thrown into boxes and then are sent to commercial storage. Rational retrieval is almost impossible because rubbish is mixed with valuable records and it is rare for box contents to be recorded in a retrievable form. The category 'Principal's miscellaneous files, 2001–4' is not helpful particularly if there are another 20 boxes labelled in the same way. Managing that process and the on–going cost is a major opportunity to demonstrate the benefits of formal records management.
- It was recently estimated by a consultancy firm that 45% of administrative staff time is spent retrieving information of one sort or another. If that time can be improved to 20% or 10% then there is a clear on–going productivity gain whose financial benefits can be calculated.

One example of a worked–out cost /benefit example is provided by the AFFIRM project, which was developed by the Western Colleges Consortium as part of a major JISC records management programme.

Crude financial measures, such as unit costing, may prove beneficial to you in the initial stages of your role particularly because some of the gains can be very large in an institution that is inefficient in its records management. What is difficult is to keep producing this level of financial benefit year-on-year as records management becomes the norm.

One further financial measure which you should consider is the costs which would be applied to your institution if you failed to comply, or were unable to comply, with the legislation and regulation under which you operate. This is not simply a matter of the financial penalties for legal non-compliance but also the legal fees and increased insurance premiums which might also be applied in particular circumstances.

In the medium and long-term you may wish to develop non-financial measures to sit alongside these. These are other targets, which reflect your own experience and needs, and to which you commit publicly. These may well include public service level agreements and performance targets endorsed by senior management. In commercial companies all these measures are brought together into a 'balanced score card', whose targets are assessed annually and if necessary adjusted. There is a very large literature on this subject. Although this method of assessing efficiency is just beginning to make an impact in UK institutions its use is more developed in the US – further information is available from [The Balanced Scorecard Institute](#)

Non-financial benefits can be summarised in the following way

Efficiency

- Information can always be retrieved quickly and reliably
- Information is available to support strategic decision making
- Access to the collective memory of an institution provides precedents for actions, and should prevent the need to 're-invent the wheel'
- Streamlined business processes (functional analysis is a core part of a systematic records management programme)
- Reduced compliance and regulatory retrieval costs
- Better utilisation of prime office space (characterised by reducing the number of filing cabinets full of obsolete paper in offices, and increasing people space)
- Reduced overhead costs of storage and retrieval of information

Competitive Advantage

- Long-term management of physical assets
- Improved public image by ability to respond quickly and appropriately to requests for information
- Ability to respond quickly to new situations

Steps Towards Good Records Management

Who should be involved?

One of your major tasks as records manager is to identify key stakeholders who have to be persuaded of the necessity and benefits of your role. There are formal ways of doing this and the Project Management infoKit has a section on [stakeholder analysis](#) that you will find a useful tool.

We suggest that you undertake some analysis of your stakeholders and their likely attitudes to your work. The Project Mangement infoKit offers a template for the analysis. Follow the link to view a [completed stakeholder analysis template](#).

There are two groups who need to be convinced above all others. Senior managers are most likely to be impressed by arguments about efficiency, compliance and costs. Your other colleagues are more likely to be persuaded by practical demonstrations that your activities will make a difference in their working situation, even if there is some short-term hassle.

Senior Managers

Once the need for records management is acknowledged Senior Managers in institutions need to take the following steps:

- Recognise records management as an important corporate responsibility and give it the appropriate level of priority and authority
- Assign overall line management responsibility for records management to a senior member of the management team
- Commission an audit of existing records management and structure within the institution (an Information Audit). This may involve the use of external consultants unless the skills already exist within the institution.
- Develop an Information and Records Management Strategy for the institution which ensures that there is an integrated approach to records management, data protection and other information management functions and procedures. Alternatively, ensure close practical liaison between them. In some cases records management will be seen as part of a wider Information Management Strategy.
- Appoint or train a person to turn the strategy into detailed policies for the institution and give them sufficient seniority to be credible throughout the institution. Many of the older and larger Universities have developed the records management function out of their historical archive units, but in most cases these now follow different reporting lines. In FE and small HEIs the role will tend to be added to those of the Data Protection Officer, the person responsible for Management Information Systems or the College Librarian.

An Agreed Institutional Records Management Policy

This is a necessary first step. Its purpose in any institution is political, to ensure the highest possible level of support for the records management process. Ideally it should be endorsed by the Board of Governors (or its equivalent) and should be actively supported by the senior executive. It should be short, and confine itself to outline principles rather than detail.



An example Records Management Policy is included here. This can be downloaded and used as a template for your own institution.

This is the key institutional document to which any records manager can always refer as agreed policy if their role or authority is challenged.

Records Managers

The Institution's Records Manager is ideally a fully trained and experienced professional. In practice, particularly in small institutions and FE colleges, that is unlikely. The job is most likely to be done by somebody who has an existing IT, MIS, or data protection role. As part of continuing professional development it would be reasonable to expect the institution to support the person through the necessary training events and courses. The major danger is an assumption that previous experience will be sufficient to deal with the whole situation without much further thought or training. Specifically, someone from an IT background may be tempted to assume that there is an over-arching IT solution to the situation. Would that it were that easy...!!

The Records Manager is responsible for drawing up guidance for good records management practice and ensuring compliance with the overall policy. The guidance should deal with:

1. Records creation
2. Filing classification schemes
3. Retention Schedules
4. Storage and Maintenance of Records
5. Final disposition of records: – historical archive or destruction. They should also be responsible for maintaining the audit trail of all records destroyed.
6. Codes of practice and legislation

All Staff

FOI impacts on all of the staff within an organisation: everybody should:

- Be aware of the role they must play in ensuring compliance with the Freedom of Information Acts and Data Protection Acts.

- Be aware that after 2005 the public may see a large number of the records created. Regularly review and dispose of files, including emails, according to the Retention Schedules.
- Keep an accurate record of activities

The Department of Constitutional Affairs has produced a new training guide, which although primarily for training staff for Freedom of Information you will find very useful in a wider context. It is comprehensive and therefore long.

Another short guide has also been produced by JISC Legal which can be found on the JISC Legal Website.

The Information Audit

Good Records Management can be seen as a cyclical process going through five distinctive phases. The rest of this infoKit will work through each of these steps, and suggest sources of further information where appropriate.



The information audit contains two interlinked elements which are of importance if the benefits of a records management programme are to be realised:

- Analysis of the business processes and systems which currently create and use information in the institution.
- The audit of the information content itself

In the first case what the programme is trying to establish is the route by which information passes through a business process; who creates it, who modifies it, who needs it, and who deals with its storage and disposition. This part of the programme is best described as a Process Review

If at all possible the person conducting the audit will attempt to deal with both elements in a single pass. However in some processes and some large organisations this will not be possible and the two elements will have to be conducted separately.

The most fully developed methodology is the DIRKS programme of the National Archives of Australia. This is an eight step process to improve record keeping and information management practices, and includes recommendations for the design and implementation of new systems throughout the agencies of the Australian government.

The scale of this is both larger and more elaborate than would be appropriate in most educational institutions but the experience and the practice it represents has been scaled down successfully to meet the needs of UK colleges. There are examples in UK FE and HE to which you can refer.

- A flexible framework for Institutional Records Management (AFFIRM) Project.
- Establishing good practice in FE records management at John Wheatley College.
- University of West of England Records Management Project.
- JISC Records Management Project for Warwick – JISC Records Management Project.

These were all part of a major JISC records management initiative which took place in a variety of FE and HE institutions during 2003 some of which looked at particular areas of record keeping for example student records and HR records. The full list and links can be found at – Supporting Institutional Records Management.

We strongly recommended that you have a look at some of these as part of your preliminary preparation work. All are practical and deal with both the triumphs and difficulties of the records audit and management process.

What's in a Name?

The Information Audit is also known as a Records and Information Survey, and in older publications may be referred to as a Records Census. Whatever the title, the objective is a comprehensive survey of all records created or held by the institution.

The word 'audit' tends to be intimidating because it is usually associated with the annual financial audit. The information audit may produce financial information, but that is not its prime purpose.

An information audit should cover all media: – paper, microfiche and electronic systems.

In some guidance a distinction is drawn between an Information Survey which concerns itself only with information processing and current records, and a Records Survey which concerns itself with semi-current and 'old' records. For the reasons stated in the Lifecycle of Information section this is unlikely to be a useful practical distinction, and it is not a valid legal distinction.

Why Do an Information Audit?

The Information Audit provides an objective assessment of an institution's record keeping practices, and the way in which that information is actually used. 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 aspects of the business (including those that some might prefer to keep hidden).

- It is likely to highlight where there is unnecessary duplication of records
- It is likely to indicate where business processes might be streamlined for more efficient administration
- It is likely to show up where records are kept too long
- It is likely to highlight filing cabinet 'fiefdoms', where information is treated as a personal asset to be shared grudgingly rather than as a resource to be shared by all as needed

- It is likely to highlight what genuinely needs to be confidential and what does not
- It is likely to show where there might be cost savings

The methodology and rationale is very similar to undertaking a process review. More detailed information can be found in the [Process Review infoKit](#).

Finally it is a clear example of rational and good management practice and an important element of good corporate governance.

Where to Start

The approach required for success in the audit will depend upon the size and structure of the institution. A large multi-site, multi-school university with a devolved management structure will require a different approach from a small college with a tight, centrally controlled management structure. This is not just a matter of scale, but a fundamental difference in the way in which each goes about its daily business.

However in either case a single person or very small team will be made responsible for the task. In an ideal world, that person will be a professionally trained Records Manager (for whom this infoKit is in the 'Grandmothers-and-eggs' category) but the smaller the institution the more likely it is that it will be a task added to an existing role as an IT Manager, data protection officer, information professional or Management Information officer.

Whatever the starting point, the audit needs to be pre-planned carefully. This should include:–

- A clear commitment and support from senior management
- A clear list of objectives
- A communication strategy
- Collection and processing of the data gathered
- Design and completion of forms

Senior Management Commitment

Enough has been said in the Steps Towards Good Records Management section to indicate that without Senior Management commitment the audit is likely to fail. At best it will be incomplete. The only reasons for undertaking a partial audit are:

- To demonstrate to senior management that there are some 'quick wins', which have immediate and tangible benefits. This is part of the persuasion process. Success here relies on careful selection of the area to be audited.
- A preliminary test of the indicative cost/resource requirements of a full-scale audit.
- A training exercise for those involved in the larger audit.

We recommend that you view the audit as a project and use a structured approach to achieving the planned objectives. The [Project Management infoKit](#) gives advice on how to achieve this.

Objectives of the Information Audit

The information audit has a series of specific objectives. These can be divided into immediate, short term and long-term objectives.

Immediate

- An interim report on the current state of play, which is non-judgemental and allows the process owners to confirm, amend or refute your preliminary conclusions. It is an overview, whose outcomes will shape the way you go about the detail of the audit. In many situations these will be accompanied by process maps which allow you to go back to your informants and say, 'this is what I think happens in your area, is it correct?' This is probably the vital stage for achieving willing buy-in from your colleagues. It is also an important element in a Communication Strategy.

Short-term

- To establish the shape of the organisational structure
- To identify which business functions create which records
- To identify what these records are used for
- To identify where they are kept and by whom
- To identify how long they are kept and how long they should be kept
- To identify who needs to use them now, and who might need them in the future if the present record holder leaves the institution, or if the structure of the organisation itself changes.
- To identify legacy systems and records which might be discontinued
- To identify vital records, that is the small core of records which are necessary for the institution's daily business and legal obligations. It is vital that these records remain accessible whatever disasters occur.

Long-term

- Development of economic records storage and retrieval
- Improvement of records management systems
- Development of improved work-flow processes
- Development of retention schedules (also known as disposal schedules)

In practice in almost every case it is the short-term which will determine the approach and the priorities.

The Information Audit – A Health Warning

There is no single approach or theoretical methodology which will guarantee success in the information audit. In an ideal world it would be an on-going process which is steadily up-dated across time. This would prevent staff and systems slipping back into more easy-going ways. Practical experience suggests that a fixed period repeat of the exercise, say every 2–3 years, is necessary to keep everything on track and to accommodate changes in organisation, business processes and personnel.

There is always a possibility that you will find something which runs counter not just to agreed records management policy but is more fundamentally against institutional policy or is simply illegal. General advice here is useless because the circumstances will be specific and there are likely to be ethical choices to be made. From a purely self-defensive point of view it is vital that you do not collude in any cover-up, no matter how important the offender, because it will come to light. In a Freedom of Information regime this will be sooner rather than later and you will be castigated as an accessory (the person who knew but did nothing).

It is more likely that you will make your recommendations but for a variety of reasons, some good some bad, nothing happens. How do you deal with this? It is possible to jump up and down and although you may win the immediate battle you are likely to create opposition by this tactic and resistance to your proposals. Records Management is a long game, and the experience of this writer is that most problems come around again in time. Having a ready made analysis and solution to the situation is usually

welcomed. Successes are your cumulative credit. Reasonableness and impartial advice coupled with professional competence usually means that in time you will be trusted to come up with the best solution for everyone.

It is worth undertaking a risk assessment at the start of the process. The [Risk Management infoKit](#) covers this and provides a template for assessing risk. A [completed example](#) is also available.

An over rigid or theoretical approach is likely to be counter-productive for three reasons:

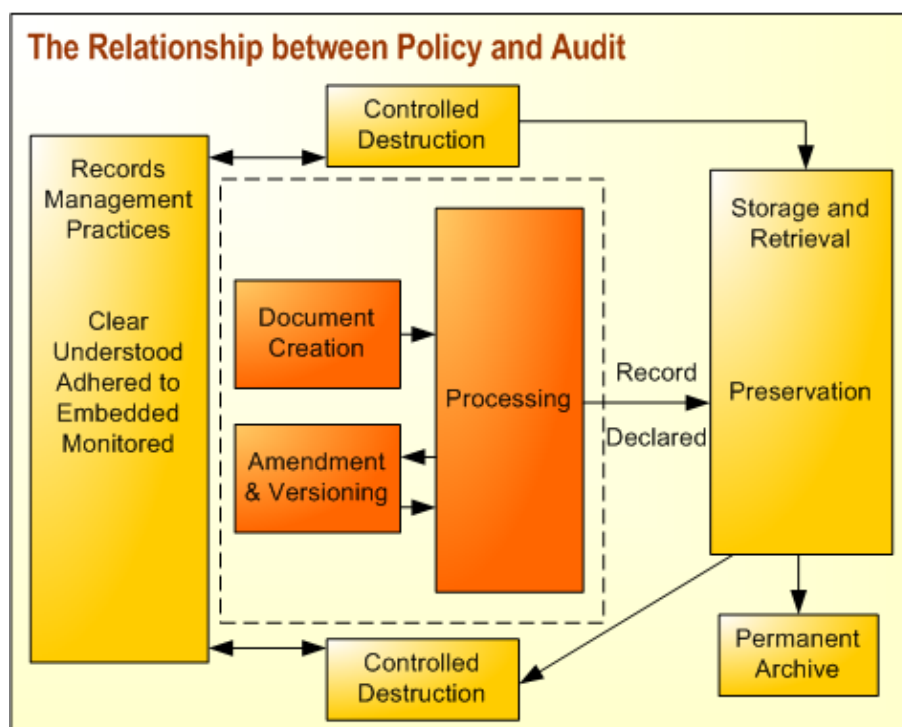
- It is likely that important records will be missed or their importance undervalued because they do not fit the pre-existing agenda.
- There will be a tendency to 'hide' the untidy or inconvenient. From the point-of-view of the objectives outlined this will be self-defeating.
- Even if the policy is implicit rather than explicit it is almost always noticeable to those at the front line. This will limit willing co-operation. Hidden agendas create reservation and fear. It is vital to have staff 'buy in'.

Above all it is a people issue. It is vital that whoever is tasked with carrying out the audit communicates with colleagues, and brings them along with the objectives. The approach should emphasise the 'carrot' rather than the 'stick'. If at all possible an identified 'quick win' which makes a demonstrable difference to working situations will produce co-operation which no amount of fine theory or exhortation can match.

The approach should be as open-minded as is consistent with achieving the objectives outlined in the section **Where to Start**.

The Relationship between Policy and Audit

Across time the Audit and Destruction practices should feed back into the institution's records management practices and produce modifications. If necessary these can in turn feed back into institutional policy.



The Starting Point

Whatever the formal title of the person made responsible for conducting the audit, a number of preliminary tasks will need to be done:

- Obtain, or draw up, a plan of the institution's existing management structure and identify the key players who can be helpful and who should be involved. Keeping this group informed of progress both formally and informally is a key element in a successful audit.
- In a large institution it may be useful to identify champions in particular schools or departments, who can be brought together to discuss issues, and who can help at the gathering information stage.
- Draw up a preliminary plan, with a rough idea of timings and costs (this will certainly be modified as the audit progresses).
- Identify known storage areas for 'old records'.
 - ◆ Do not start with these. Always start with the current business structure and processes.
 - ◆ It is almost certain that the majority of records in store will form part of working series and sequences that are easier to identify from current business practices than in isolation.
- Your work will begin in the same way as a Process Review.
- Draw up a formal Project Management plan for the audit to control timings, effort and key stages. You can get more information on how to do this in the Project Management infoKit. This has the advantage of being able to give particular departments or schools both an indication of priorities and the probable date of the audit reaching their patch. It has the additional advantage of helping to avoid disruption to business at difficult times. For example, no Finance Department would welcome the audit during the annual financial audit. It permits timings to be negotiated, and if necessary, changed without disruption to the overall schedule.
- Identify two or three quick wins, probably in the central administration. This has two purposes:
 - ◆ Political – to give a demonstration of what is possible
 - ◆ Practical – to try out a do-able part of the audit as a method of testing techniques. This will show up where the methods need modification.

You should have a look at the Appendix to the Study of the Records Lifecycle. It gives an indication of the general headings and categories of record which might be expected in particular areas of a college or university. It will also help to shape the questions which should be asked as part of the audit.

A Communication Strategy

During the course of the audit, which may take many months, it is important to keep all stakeholders informed about, and happy with, the progress. A well-developed communication strategy, using all available methods, is vital.

1. A general statement to all members of staff explaining that the information audit is to take place and why it is in the interests of everybody that it should be done properly. This should have the full support of senior management and should be short and to the point.
2. Regular communication beforehand with those who are acting as the local contact/champions. Initially this might involve a training session/discussions and telephone calls. Later an informal newsletter or feedback to this group as the audit progresses whether or not they are directly involved at that point in time.
3. Direct communication with the area, department, school or unit before the audit is scheduled to take place. After it is completed give feedback with some preliminary suggestions and conclusions.

4. Regular Progress Reports to Senior Management even if this is not formally required as part of the task. This is a vital element for ensuring continued support and, if need be, resolving disputes, or difficulties.
5. Regular general bulletins to all members of staff containing general news, wins, or fascinating facts unearthed during the audit are important in winning over the unconvinced. This can be done through existing news bulletins which most institutions issue or via the intranet. Short and snappy is the general rule.

How to Go About Information Gathering

There are a number of possible approaches to the task of getting the necessary information:

- A formal questionnaire
- Selective, but unstructured, interviews with members of staff
- Structured interviews with key members of staff

Practical experience suggests strongly that the scattergun approach of a questionnaire to all members of staff has a small success rate. Response rates of less than 20% are very common.

An unstructured interview almost certainly means that items will be missed, forgotten or ignored as 'not being important or relevant'.

The structured interview with key staff, almost certainly the people responsible for Departmental, school or faculty administration in the first instance, will give the whole exercise a shape and will also provide the leads to other important sources of information within the same area. This should be allowed for in the project plan, and if used carefully, is not a bad way of proceeding. It also allows a single department/faculty/school to be dealt with in a single pass and the audit process to move on elsewhere in the institution.

The Questions to be Asked

The questions should be phrased in such a way as to evoke a yes/no or purely factual answer. It is very important to think through carefully the questions which need to be answered. They have to be related to the purpose of the survey and the way in which the results will be used. There is no standard format for this, and some questions which might be highly relevant to one audit could be equally unimportant in another.

On the other hand the audit is a one-off opportunity which cannot be repeated very quickly, so it should be as comprehensive as possible. The most economical way to deal with this is to set it up as a table in a database. This would allow some of the preliminary analysis to be done using the properties of the database. We have provided a template of the way this might look and an example. However the template offered in this infoKit is not intended to be comprehensive. There are matters which every institution will want to add as part of its audit.

The Physical Inventory

The physical inventory starts with the identification of all the places used in a department for storage and the equipment make and model being used. This will include filing drawers, cabinets, cupboards, and locations where the department reckons to store material off-site. You should record this as the audit progresses.

Equally important is to have a look at all PCs, note how and whether they are networked, the packages

used and the existing ground rules for e-mail and internet use. Some institutions will already do this type of auditing as part of their IT function and the information will be available. In many cases such equipment will be included in the central asset management register which should be easy to access. This will, among other things, tell you when equipment was bought and therefore how old it is and where it sits on a probable replacement cycle.

In either case close collaboration and support from IT colleagues will be vital.

Next Steps

Analysis of the returns from the information gathering stage will quickly reveal:

- Areas where the business processes are being supported adequately by record keeping.
- Areas where changes will have to be made because external statutory or regulatory requirements are not being met.
- Areas where records management processes are haphazard and where a regular system must be introduced.
- Areas where business could be improved by simplifying a procedure.
- Areas where the record, and therefore the institution, is at risk.

The major task is to create a report defining what is required to ensure compliance with all legislation and regulations.

The second step is to draw up a Retention Schedule for all types of record encountered. It is to be expected that in larger institutions different practices and standards will prevail in different parts of the organisation. It is vital from the point of view both of Freedom of Information and Data Protection that these are standardised across the institution, agreed and enforced. See the section on **Records Retention Schedules**.

Finally it is useful to suggest how long records might usefully remain in a working area or current file for current business purposes and when they could safely be moved to semi-current storage. The aim is to keep the current working area and systems as uncluttered as possible and focused on the immediate business.

Electronic Records

Is there a difference?

Electronic records require all the same care that should be applied to records on paper or captured on microfilm but present some unique and difficult additional challenges. The key difference is that the appropriate index terms, search data and retention period (usually referred to as **metadata**) have to be applied at the point of creation if there is to be any chance of finding the record again or managing it as a record in any rational business system.

Electronic Records are:

- Easy to change, copy and modify
- Complex and tend to lack a clear structure when being created
- Fluid
- Transient and need positive decisions for selection and preservation at the very start of the life cycle.

Copy or Original Record?

A record, which is created electronically as the only record of a transaction, decision or activity is an original record. It is worth saying that the final word processed version of a document held in an electronic system whether it is a minute or a letter is the original not the paper version.

A record, which is created electronically as a facsimile or digitised version of a record created in another medium (paper, film, voice) is a copy record. This remains true whether or not the original still exists.

Objectives of Electronic Records Management

There are three core objectives which must be applied to each and every new electronic record:

- **Authenticity.** It must be an accurate version of the activity, transaction, or decision it represents
- **Integrity.** The record must not be altered after it has been created or 'declared'. As a general principle if the record content/information is required for subsequent processing this should be copied and a new record created.
- **Non-Repudiation.** The original ownership of the record must be established and maintained to prevent the originator from disowning the record.

Electronic Records Management Policy

This must cover five principal areas;

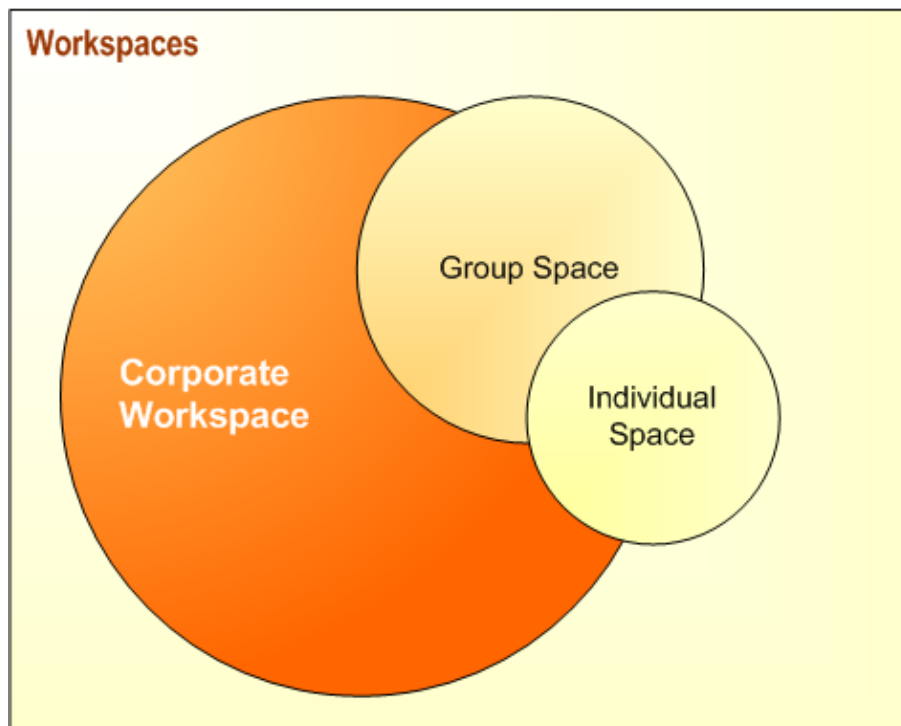
- Capturing electronic records into an Electronic Records and Document Management System (EDRMS) where one exists within your institution. JISC infoNet has a separate applied infoKit on implementing Electronic Records and Document Management Systems.
- Designing appropriate indexing, search-terms and reference information (usually referred to as metadata) for application as the record is created. This is the most vital step of all because without it recovery of the record from systems will be virtually impossible after a very short period of time. The electronic Bermuda triangle where data is added to a system and then is irretrievable is a very well-known phenomenon.
- Keeping Records safe and accessible. This involves identifying Vital Records, updating offsite and security copies, ensuring that data transfer is a fully certified and documented process and ensuring that security copies also meet the requirements of Freedom of Information and Data Protection legislation.
- E-mail management and use
- Retention and Preservation of Electronic Records. This is perhaps the most little understood part of policy because it is an area in which IT specialists have traditionally been over-confident in their ability to find a technical solution when it is needed. They may be right but prevention is cheaper than cure. By way of warning about the survival rate of electronic records storage media the **Digital Preservation Coalition** has produced the following table of life expectancy of various electronic storage media under different conditions of temperature and relative humidity.

Device	25RH 10°C	30RH 15°C	40RH 20°C	50RH 25°C	50RH 28°C
D3 Magnetic Tape	50 years	25 years	15 years	3 years	1 year
DLT Magnetic Tape Cartridge	75 years	40 years	15 years	3 years	1 year
CD/DVD	75 years	40 years	20 years	10 years	2 years
CD-ROM	30 years	15 years	3 years	9 months	3 months

By way of contrast paper documents that are kept at a temperature of 16–19 degrees celcius and a relative humidity between 45–60% should be good for 100 years plus (British Standard 5454:2000).

Good Housekeeping and Making Better Use of Investment

There are a number of features of many existing record–creating electronic systems which offer some records management advantages. Most users operate in two or three distinct areas. Work PCs are normally linked in a group workspace, which may in turn overlap or be linked to a corporate workspace.



In practice this means that many staff are already used to the idea of working in a common space whose files have to be labelled in such a way that all can find them easily. The levels of permitted access are controlled either by a local system administrator, or in the corporate space by the central IT management.

This gives the opportunity for rule–based records management, and a degree of central control. The key to success is staff training.

The policies need to cover

- An agreed File Plan for shared file areas. In an ideal records management system this would be based on function, the creation of new folders would be strictly controlled, and file naming conventions would be agreed.
- MS Office documents.
 - ◆ The document properties box can be used to improve metadata
 - ◆ Documents can be 'declared' as records by using the 'read only' tag
 - ◆ Standard templates can be used to improve form design
- Version control of documents.

We have an example of how an MIS project team applied records management to its file storage.

- The selection of new record-creating systems, for example finance or web content management systems, should include
 - ◆ functionality for records preservation
 - ◆ the generic specification for answering FOI, Data Protection and Environmental Information queries. The Department of Constitutional Affairs has included a specification on the Directgov Website

E-Mails

The control and management of emails is a very large and controversial subject which cannot be pursued in this infoKit. It is however important to remember that it is the information content of the e-mail which is important and may need to be retained rather than the fact that it has arrived as an e-mail.

There are however a number of key issues here, which need to be incorporated into any institutional E-mail Policy, such as:

- ◆ Who owns e-mails, the institution or the recipient, or is ownership shared according to content?
- ◆ Where does responsibility lie for capturing e-mails, the recipient or the institution?
- ◆ Should all e-mails be eliminated automatically at x weeks unless they have been specifically saved to agreed files?

E-mail policy is perhaps the most tricky area that all institutions will need to sort out under the new Freedom of Information and Data Protection regimes. Most will have some guidelines in place but very few have tackled the issue head-on. For most institutions it is the area where personal and business considerations overlap in a very untidy way and the sheer volume of traffic seems to make central intervention both cumbersome and an infringement of staff autonomy. There has been one JISC study of this matter – Institutional Records Management and E-mail. The important thing to remember is that e-mails are available for Freedom of Information searches irrespective of the wishes or opinion of the creator.

There are a number of choices that have to be made when building an e-mail Policy:

Ownership

- ◆ All e-mail messages belong to the institution
- ◆ Only business messages are owned by the institution
- ◆ Personal messages are owned jointly by the institution and recipient or writer
- ◆ Personal messages are confidential

Permitting e-Mail Use

- ◆ E-Mail may be used only for the institution's business
- ◆ May be used for incidental personal purposes

- ◆ May be used for all purposes without restriction

Labelling

- ◆ All personal messages must be labelled as such
- ◆ Messages must disclose the limits of the employee's authority
- ◆ Personal messages must carry a specified disclaimer

Monitoring

- ◆ E-mail may be monitored for any business purpose without notice or consent. (This is unlikely to be permissible under Human Rights legislation)
- ◆ Monitoring permitted with good cause or legal obligation
- ◆ Agreed procedures for monitoring
- ◆ No monitoring

Contents Disclosure

- ◆ Message contents may be disclosed for any business purpose without consent
- ◆ Disclosure as required by law
- ◆ Agreed procedures for disclosure
- ◆ No disclosure

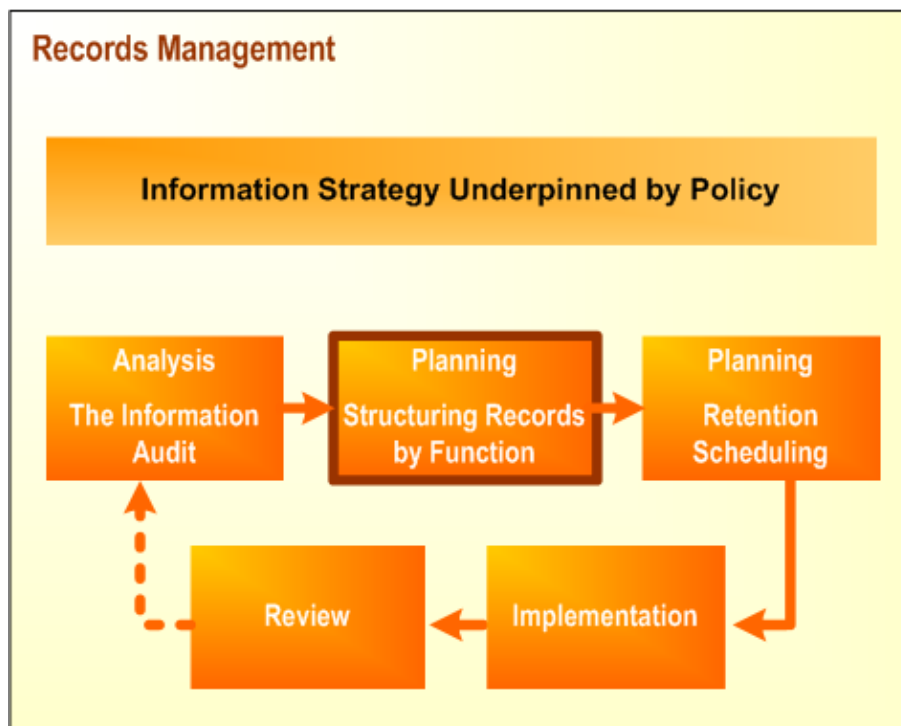
Substantive Rules

- ◆ System may not be used for illegal or wrongful purposes
- ◆ System may not download software without technical approval and vetting
- ◆ System may not be used for electronic snooping.

You can view Northumbria University's [e-mail use policy](#) and [good practice guide](#).

Functional Analysis

This is the second of the five phases of the records management process.



It is worth re-emphasising four points which have been made already:

- Records Management and the audit is a corporate responsibility. One of the long-term objectives of the information audit is to ensure that different areas of the organisation handle records with the same function in exactly the same way and according to identical criteria. Specifically, student records in faculty, school or department x need to be dealt with in exactly the same way as those in Y. The larger the College or University, and the more devolved the management structure, the greater the likelihood of significant variations in practice.
- Although you will have gathered the information according to the existing organisational structure of the institution, there is no need to organise your findings in this way. You will find that the function of admitting students is more or less the same business processes throughout your institution. It is obviously better if everybody uses the same terms for this process, since this is one category of information that is likely to be shared. Put simply, your analysis of the information received will be made according to the purpose or function for which the record was created rather than by the department which created it.
- Some elements of this approach to record keeping already exist in the e-systems of most institutions. The development of workspaces in servers which can be shared by a group of co-workers fundamentally requires an agreed naming structure for files, and agreed management processes.
- One other reason for approaching the task in this way is that although the organisational structure of your College or University will change (for example when departments merge) the fundamental reason for creating the record tends to be unchanged. Those functions which stop with organisational change can simply become 'closed' records series, while those that continue show that underlying continuity. It also means that there does not need to be constant revision of the structural plan for records, because most new record types can be accommodated within the existing structure. If a completely new function is created this can be added.

This way of looking at the record classification process is fundamental to successful records management and is usually designated functional analysis. It is the key tool for achieving intellectual control of an institution's records and the business processes which created them.

The usual term used to describe the output from this is a **corporate file plan**, and the agreed naming conventions the **taxonomy**.

Advantages and Disadvantages of Functional Classification

In the 'bad old days' before electronic systems swept all before them, many organisations had a registry which controlled, named, tracked, retrieved and stored paper files and was staffed by file clerks. Success depended upon the skills and care of the organisation's administrators but in practice this was often variable. It did mean that with suitable permissions and controls many members of staff could share the information that the files contained (although not simultaneously). Electronic systems, especially desktop PCs, did away with all of this, but did not really replace it with anything comparable. It was not thought necessary. Changed days have changed requirements. One way of looking at a corporate file plan is as technique for re-asserting control over corporate information assets.

Advantages

- The Model Publication Schemes to which most Universities and post-16 Colleges in the UK have signed up are organised by function. It was the only way in which such templates could be devised given the great variety of organisational structures. The main functional high-level categories in Scottish Higher Education are:
 1. GENERAL INFORMATION
 2. ACCESS TO INFORMATION
 3. GOVERNANCE

4. FINANCIAL RESOURCES
5. CORPORATE PLANNING
6. PROCUREMENT
7. MANAGEMENT OF RESEARCH
8. COMMERCIALISATION AND KNOWLEDGE TRANSFER
9. HUMAN RESOURCES
10. PHYSICAL RESOURCES
11. HEALTH AND SAFETY
12. SUPPORT FOR DISABLED PEOPLE
13. STUDENT ADMINISTRATION AND SUPPORT
14. TEACHING QUALITY
15. INFORMATION SERVICES
16. EXTERNAL AND COMMUNITY RELATIONS
17. GOVERNMENT AND REGULATOR RELATIONS

The Colleges' version is very similar except that Category 7 has been removed. JISC Legal's [website](#) gives the links both to those for Scotland and the rest of the UK.

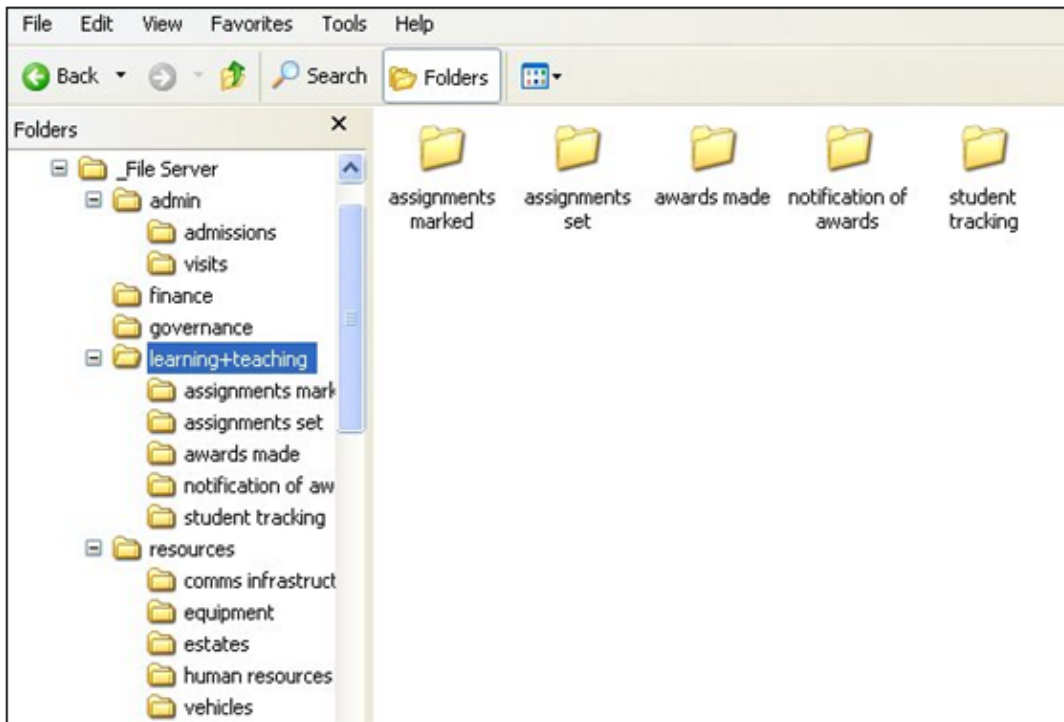
- Functions do not change over time
- Files can be easily identified and used without affecting the fileplan classification
- There is a greater spread of ownership
- There is better search and retrieval of information
- The transition from paper to e–systems becomes simpler and more transparent
- New functions can be added
- Work processes are identified and mapped
- A fileplan and taxonomy has to be devised as part of the preparation for [electronic document and records management systems](#)

Disadvantages

- Implementing such a system across an institution requires a cultural shift in the organisation and attitudes. It also requires confidence in the systems in place. It is both an organisation and a people issue.
- To the 'first–timer' the relationship between the organisational structure in Departments, schools and faculties which is easily understood does not relate immediately to the corporate file structure by function. This appears to be an intellectual abstraction rather than a business tool. The curious thing to say is that once in place such a system it becomes almost second nature, because it removes the uncertainty of 'What shall I call this, and where shall I file it so that I can find it again?'
- The major hurdle to be overcome is the perception that work is 'my work' rather than part of a bigger business process which must be shared (and in practice usually is). The key is not who owns the work, but how the work is done.
- Older ways of organising files by subject, creator or department become irrelevant, and the feeling of personal loss of control of file taxonomy has to be counteracted by making it easier to retrieve and share all information.

Functional Classification – A Practical Example

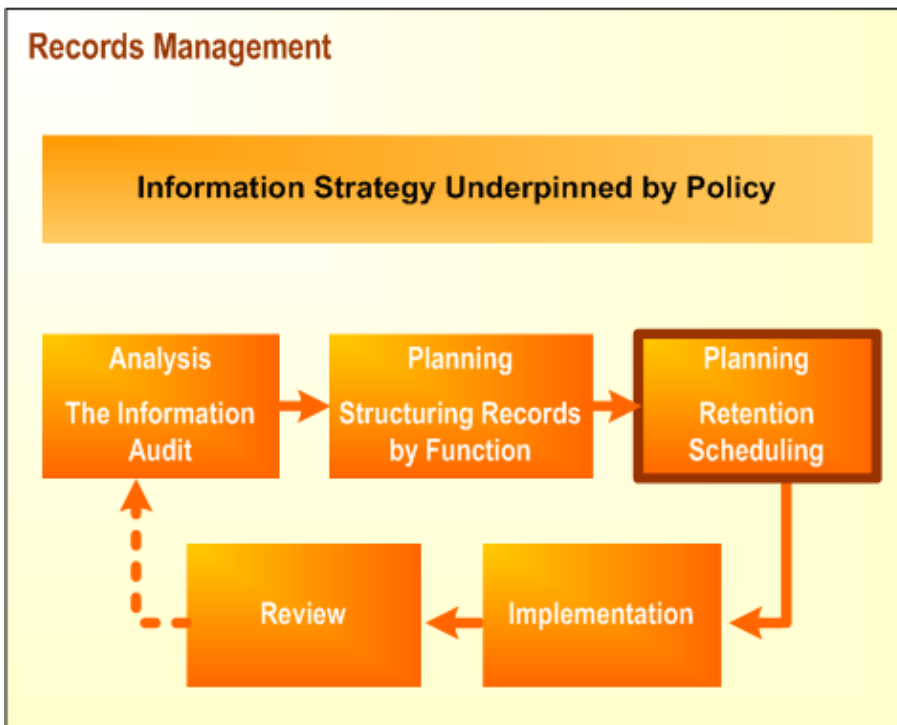
Consider function 13 Student Administration and Support. This will have a series of sub–functions under it such as 'student admissions' or 'learning and teaching'. This in its turn will be sub–divided into a number of activities such as 'assignments marked', 'assignments set', 'student performance tracking' and so on. At this 3rd level it is possible to leave a good deal of flexibility provided it fits within the overall structure of the function and sub–function. To a person operating in such a system the filing structure available on–screen from a shared drive might look something like:



Two JISC studies are worth looking at in more detail for practical examples in a Further Education context. The [Model Action Plan in an FE context](#) and [A Flexible Framework for Institutional Records Management](#).

Records Retention Schedules

This is the third of five phases in the records management process.



A retention schedule is a list of records for which pre-determined destruction dates have been established. It is also known by a variety of other names including disposal schedules, and destruction

schedules. The aim of the information audit is to establish those categories of records for which there is a known disposal date. The Retention Schedule brings all this information together in a single report.

It has three objectives:

- disposal of those records which have completed their retention period
- storage of records which have to be kept temporarily after they are no longer needed for current business
- preservation of records which are of long-term or historic value

In practice the schedule will have dates varying from a few months to permanent retention, as outlined in the section on retention periods.

Practical examples of the retention periods required in FE and HE by law and statutory regulation is to be found in '[The Study of the Records Lifecycle: HEI Function and Activity Model](#)'.

An example for just one small area in an HE institution looks as follows:

6. The Retention Schedule

University Process	JISC Generic Record Retention Schedule			University Practice	
	Ref	Description	Retention Period	Retention Period	Official Copy Holder
Assignment Set	1.15	Records documenting the development of taught course assessments	Life of course		Academics
	3.16	Records documenting the development and establishment of the institution's assessment and examination rules and procedures	Superseded + 10 years		Registrar
Assignment Published	1.15	Final versions of taught course assessments:	Life of course		Academics
Students submit completed Assignments	3.15	Schedules for submission, marking and return of coursework	Current academic year + 1 year	December after current year	School Admin
	1.15	Taught course students' submitted/completed assessments:	Current academic year + 1 year	December after Resit Board	School Admin
	3.15	Records documenting individual students' submission of coursework	Current academic year + 1 year	December after current year	School Admin
	3.16	Records documenting individual students' submission of assessed work and handling of reports of mitigating circumstances	Current academic year + 1 year	Copy to Student file (originals) – retention could be 4/6 years	School Admin
Assignments marked, assessed, moderated, recorded, published	1.15	Records documenting marks awarded to submitted/completed assessments, including reviews in response to notifications of mitigating circumstances and academic appeals.	Current academic year + 6 years		Central Admin/IT Services
	3.13	Records documenting the handling and results of academic appeals by individual students	Last action on case + 6 years		School Admin
Awards made	1.15	Records documenting awards and classifications	Current academic year + 6 years		Central Admin/IT Services
Notification of Awards; Final Record	3.16	Records documenting the issue of awards lists and individual notifications of awards.	Current academic year + 1 year		Registrar
	3.16	Records documenting the collation of examination results and compilation of pass lists and individual notifications of results	Current academic year + 1 year		
	3.16	Pass Lists/Awards Lists	Issue of List + 10 years		

This example is taken from the JISC project on Student Assessment records at Northumbria University.

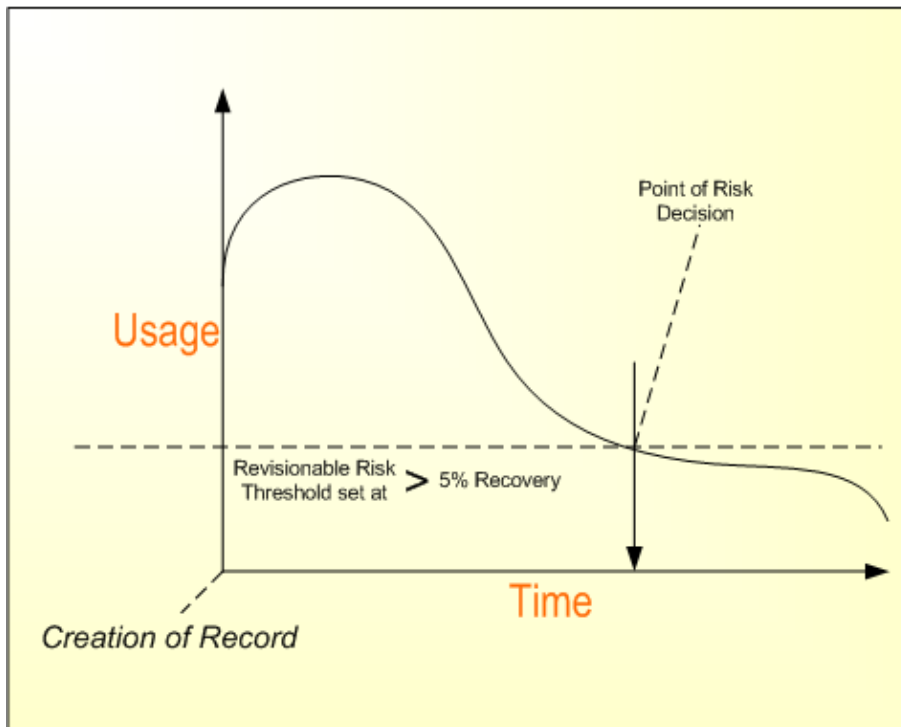
Risk Assessment

There will be a number of significant records for which there appears to be no clear-cut period of years for which the record has to be maintained.

There are two ways of dealing with this problem.

- Conduct a risk analysis on the probability of the record being needed against risk of the cost to the institution of the record not being recoverable. Then the retention period would be determined on the basis of reasonable risk. Broadly speaking demand for any class of records tends to follow

a similar pattern, which if plotted on a graph tends to look as follows:



There will be a point at which demand for use drops below the defined threshold which can be set by the institution. A decision can then be taken on the basis of probability of recall against the consequences of not being able to produce the record.

- The second option is to mark all material which cannot be given a definite retention period with a 1st and 2nd review date. Typically these might be set at 3 and 6 years, or 5 and 10 years. The 2nd review should be the point at which it is possible to determine whether it is necessary to keep the records permanently i.e. 30 years plus, or whether they could now be destroyed.

As a general point of good practice it is probably wise to have a system that where there is a clear-cut retention period the record is disposed of without further consultation.

Most of the JISC projects previously cited contain detailed information about retention periods usually taking the Study of the Records Lifecycle as the starting point.

An example from a planning and strategy function of a large University can be found at [A records lifecycle for planning and strategy functions](#).

Another example relating to employee records can be found on the [JISC website](#).

The only exception to this rule would be new legislation, applied retrospectively, which effectively alters the retention period. For this reason it is sensible when choosing a records management system, or developing one in-house, to allow for global changes to this data field.

Where material has to be reviewed after a period of years it is sensible to consult. Experience suggests that those consulted will be cautious. The 'just in case' mentality is normal. One criterion which should be considered is how often the record has been retrieved and whether there is any definable pattern.

Vital Records

Vital records are those records essential to the functioning of a college or university. They are those records that protect the interests and rights of the institution, its staff, students and other major stakeholders. As a matter of course they are likely to include current year financial information, records

relating to current students and those relating to staff benefits, insurance, pension rights, proof of ownership, legal proceedings, and decisions.

With very few exceptions vital records should be duplicated and should be stored away from areas where the originals are being used. If these take the form of computerised records then they should be up-dated regularly as part of the normal back-up process and stored outwith the main processing and network areas.

Some vital records will be identified as part of the Information Audit but it really requires a distinct programme to bring the elements together fully. The objectives are:

- To define the vital records
- To ensure Senior Management buy-in
- Identify potential hazards
- Designate appropriate protection methods
- Select appropriate storage sites and methods
- Develop operating procedures
- Bench Test programme procedures

Disaster Recovery

This is a distinctive and large-scale subject in its own right. In essence it is about pre-planning to recover the business of the institution in whole or in part if the worst happens, whether fire, flooding, accident, bomb or any other hazard. The main task is to prepare a disaster recovery plan and test it. It is usually an institution wide exercise and involves technical expertise of buildings, systems and controls as well as records management. It is not a one-off exercise but one that has to be up-dated regularly. It is likely that the records manager will be a member of the core recovery team but it would be unusual for this person to have responsibility for the whole plan.

Controlled Destruction

Records that have completed their retention period should be sent for destruction. From a managerial point-of-view it is better not to give the creators of records a second chance to review disposals unless:

- There has been a change in the law or in the institution which requires a fresh look at the retention period
- There is uncertainty
- There is a potential re-evaluation of the long-term importance or a particular class of records

Where the matter is clear-cut it should be an automatic procedure:

- It is necessary to keep a record of all records disposals. This is an essential audit trail.
- All records must be disposed of appropriately. In the case of sensitive or confidential paper records this must mean shredding or pulping. In the case of microfilm this will mean grinding, and in the case of electronic data ensuring that it cannot be recovered.
- Increasingly waste disposal is hedged about with environmental regulations and all disposal practices must be compliant with these.

It is very important the list of records sent for destruction is kept (the **disposal schedule**). Under the Freedom of Information regime this is the definitive proof that disposal of records is taking place in a controlled manner. As a general principle it is sensible for the records manager, or whoever is designated to control the process, to sign off and date the destruction schedule as proof that the records are no longer in the institution. A copy of the invoice from the waste company can then be attached to the

schedule to show conclusively that destruction has taken place.

In many ways the easiest option for an institution is to use a commercial disposal firm for the disposal of paper and microfilm because their practices will be controlled, audited, and fully compliant with current environmental regulations (their business can only exist if they are). They will be able to issue a certificate of destruction that should be maintained with the disposal schedule as proof that the record has been destroyed. In the context of both Data Protection and Freedom of Information legislation in the UK these sorts of procedures are the clear proof of controlled destruction of information that the Information Commissioner would be looking for in any disputed request which the institution was unable to answer.

Implementation and Review

The fourth and fifth phases of the records management process may be considered together.



If as we have suggested the information audit, functional analysis and retention scheduling have been treated as a project or series of projects it is important both to implement the new policies and procedures, and at the same time review what has been achieved. The reason for running the two together is that the additional authority which will be needed to implement the findings of the process will be the result of a formal acceptance of your conclusions by senior management in your institution.

It is also important to draw the work done so far to a formal conclusion. The report may contain recommendations about work which still needs to be done and possible future programmes. But it is important to get a final report (warts and all) signed off.

Basically the review should look at initial aims, and check these against the actual outcomes. In an ideal world these should match exactly. In practice this is rarely the case.

The key questions which have to be addressed are;

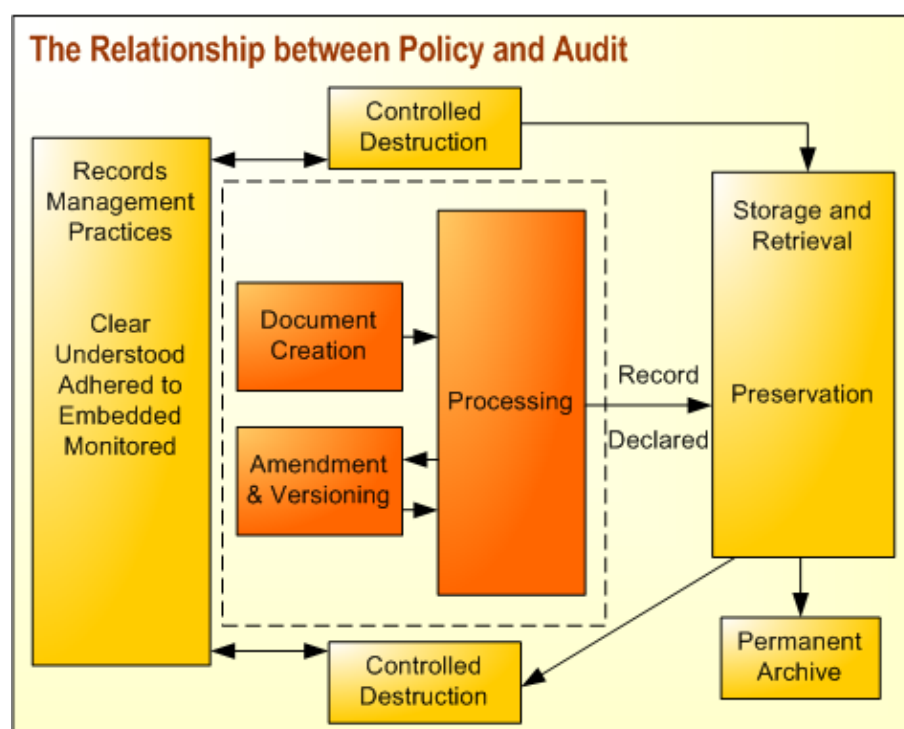
- Is the records management process working?
- Does it need modification, either at the practical or policy level?

- What still needs to be done?
- What are the problem areas?
- Are we developing systems which are fully compliant?

If the stakeholders have been informed of progress as it has happens, there should be few surprises by this stage, and either all the potential risks will have been identified and mitigated or particular risks will have been noted and isolated for special consideration.

To Conclude

The whole business of records management can be shown to sit within the larger process of the records lifecycle, and this can be shown graphically. It is important that the findings of records management feed back into policies and procedures, and possibly into the business processes which create new records.



The business of records management should be seen as an integral part of process improvement, which if achieved will produce significant and measurable gains in efficiency.

Records Management demands a wide range of skills to deal successfully with all situations. Nobody is equally skilled in every area. The key thing is knowing where to look for additional information, training or help. The writer hopes that enough has been said to make you realise that records managers in general are willing to share their experience and advice and the purpose of JISC and particularly JISC infoNet is to provide advice and guidance to FE and HE Institutions.

Further Information

Practical Experience to Which You Can Refer

During 2002–3 JISC initiated a number of practical research projects on particular aspects of records management in FE Colleges under the Supporting Institutional Records Management Programme. A number of these studies have been cited at appropriate points in this infoKit.

The following are probably the most immediately useful. The full reports will be found following the links below:

[A Flexible Framework for Institutional Records Management \(AFFIRM\)](#)

[Developing records management programmes in FEIs](#)

[Establishing Good practice in FE records management](#)

[Managing employee records](#)

[The Model Action Plan in an FE context](#)

[North Wales Records Management Consortium](#) – This was a study of the record keeping practices of HR Departments in a University and College in North Wales.

[Records Management and email](#)

[Student assessment records](#)

[What is a student record?](#)

Other Sources of Information and Training

The best way of keeping up-to-date with current concerns in the field of records and information management is to look at the JISC list-serves noted in the introduction to this infoKit, and to read the journals of the appropriate professional Societies. These are:

Journal of the Society of Archivists (Society of Archivists, UK)

Records Management Society Bulletin (Records Management Society of Great Britain)

Electronic Library and Information Systems Journal and Records Management Journal (ASLIB, UK)

Each of the above Societies runs short courses, usually 1–2 days on particular aspects of records management. Information about these courses is always available on the appropriate web-site. These are:

Society of Archivists – www.archives.org.uk

Records Management Society of Great Britain – www.rms-gb.org.uk

ASLIB – www.aslib.com

There are two main commercial have developed distance learning courses which are available in total or as individual modules. These are; Northumbria University; University College of Wales, Aberystwyth and University of Dundee.

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](#) – 2006
