

# Joined up thinking: risk reduction through Records Management

Patricia Methven

Deputy Director of Information Services  
and Systems and Director of Archives  
and Information Management

King's College London

UCISA November 2005

# Records Management: The purpose

To ensure that

- right person
- has the right information/record
- at the right time

and that records and information that are no longer required for business purposes are either destroyed or transferred to Archives

# Records Management: Scope 1

It covers all media

- parchment
- paper
- photographs
- tapes
- all digital/electronic information
- objects such as packets of seeds, examples of glass specification, models and anything else required to record information

It covers the life cycle of the information (the actual content)

- from creation and import
- to scheduled destruction or transfer to the Archives

# Records Management: Scope 2

It includes a wide range of business processes including

- registration of information/data
- mail routines
- classification (hierarchy/titling/metadata)
- filing
- indexing
- management processes for records of specific types such as minutes, patents, titles to property, websites
- management processes for the records of specific administrative functions such as personnel or finance
- licensing issues and intellectual property
- security and confidentiality (access procedures/coding etc)
- retention/destruction scheduling
- identification of information of permanent value (hundreds of years)
- methods of destruction

# Records Management: The Drivers 1

Efficiency and effectiveness in the management of business

Poor information processes and systems (whether electronic or hard copy) generate waste

- Waste of time spent looking for information or recreating it
- Waste of resources, everything from multiple copying to storing and maintaining files or redundant emails

Poor information handling generally has an opportunity cost

- If it is difficult to identify, retrieve, share and access corporate information institutions will miss business opportunities through ignorance... whether grant opportunities, new course developments or literally business opportunities

# Records Management: The Drivers 2

## Legal Compliance

- Many acts require specific types of documents or evidence to either be kept for specific periods for accountancy/audit purposes (Finance Acts) or as evidence of good/fair practice (Health & Safety and raft of equality legislation)

These acts have shaped the retention periods cited in records retention schedules.

- Others like Data Protection and Freedom of Information says less about evidence and periods of availability of information but a great deal about rights of access. The mere fact that the acts quote 40 & 20 day turnaround periods for response means that management of records and information has to be effective.

The Lord Chancellor's Code on FOI specifically mentions the need for records management. The Information Commissioner's Office has reinforced the message.

# Major legislation relevant to information security and records management

Computer Misuse Act 1990

Contempt of Court Act 1981

Copyright, Designs and Patents Act 1988

Criminal Justice Act 1988 (child pornography)

Data Protection Act 1988

Defamation Act 1996 (libel)

Human Rights Act 1998

Obscene Publications Act 1959 (pornography)

Public Order Act 1986 (incitement to racial hatred)

Regulation of Investigatory Powers Act 2000 (intercepting information)

# Computer Misuse Act 1990

[http://www.hmso.gov.uk/acts/acts1990/Ukpga\\_19900018\\_en\\_1.html](http://www.hmso.gov.uk/acts/acts1990/Ukpga_19900018_en_1.html)

There are three criminal offences under this Act:

- i) “unauthorised access to computer material” (hacking);
- ii) “unauthorised access to computer material with intent to commit or facilitate commissions of further offences” (e.g. hacking into a computer in order to commit theft by redirecting funds to own bank account, or to access confidential information in order to facilitate a blackmail scheme);
- iii) “unauthorised modification of computer material” (deliberate erasure or corruption of programs or data, including the introduction of a “worm” or “virus” into a computer)

# Contempt of Court Act 1981

It is an offence to publish or distribute anything, which may impede or prejudice active legal proceedings either accidentally or deliberately.

# Copyright, Designs and Patents Act 1988

(as amended)

[http://www.hmso.gov.uk/acts/acts1988/Ukpga\\_19880048\\_en\\_1.htm](http://www.hmso.gov.uk/acts/acts1988/Ukpga_19880048_en_1.htm)

The Act makes unauthorised copying of any copyright work (including records) an infringement of copyright, unless it is covered by one of the exemptions included in the Act. The consent of the copyright owner is required for the copying of copyright material. Where electronic records are involved the software as well as the content of the records may be subject to copyright, and the two may be owned by different parties.

# Criminal Justice Act 1988

[http://www.legislation.hmso.gov.uk.acts.acts1988/Ukpga\\_119880033\\_en\\_1.htm](http://www.legislation.hmso.gov.uk.acts.acts1988/Ukpga_119880033_en_1.htm)

It is a criminal offence to distribute, possess or advertise indecent photographs or pseudo-photographs of children under 16. A pseudo-photograph is “an image, whether made by computer graphics or otherwise, which appears to be a photograph”.

# Data Protection Act 1998

<http://www.hmso.gov.uk/acts/acts1998/19980029.htm>

The **Data Protection Principles** state that personal data shall be:

- Obtained and processed fairly and lawfully, and shall not be processed unless specific statutory conditions are met
- Obtained only for one or more specified and lawful purposes, and not be further processed in any manner incompatible with those purposes.
- Adequate, relevant, and not excessive in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up to date.
- Held no longer than is necessary for the purposes for which they were obtained
- Processed in accordance with the rights of Data Subjects, including the general rights to access information held about them and where appropriate to correct or erase it.
- Kept securely and safely, with appropriate measure to prevent unauthorised or unlawful processing of the data.
- Only transferred to a country outside the EEA if that country has an adequate level of protection for the rights and freedoms of Data Subjects in relation to the processing of personal data.

# Defamation Act 1996

<http://www.hmso.gov.uk/acts/acts1996/199603.htm>

What is libel?

- Libel consists of a defamatory statement or representation in permanent form, e.g., statements in books, articles, newspapers, letters, e-mails or on a Web page.
- Every repetition of the libel is a fresh publication. As a result, not only the author of an article, but also the editor, printer and publisher are potentially liable, although they may be able to rely on the defence of innocent dissemination.

# Human Rights Act 1998

<http://www.hms0.gov.uk/acts/acts1998/19980042.htm>

This Act incorporated the European Convention on Human Rights into English law. Of particular relevance are Article of the Convention, which give everyone a right to respect for their private and family life, their home and their correspondence, and Article 10, which grants everyone the right of freedom of expression.

# Obscene Publications Act 1959

It is an offence to publish an obscene article or item. An article shall be deemed to be obscene if its effect is, if taken as a whole, such as to tend to deprave and corrupt persons who are likely to read, see or hear the matter contained or embodied in it.

# Public Order Act 1986

It is an offence to

- Display written material, or
- Publish or distribute written material, or
- Distribute, show or play a recording of visual images which are threatening, abusive or insulting and are intended to, or are likely to, stir up racial hatred. “Racial hatred” means hatred against a group of persons in Great Britain defined by reference to colour, race, nationality (including citizenship) or ethnic or national origins.

# Regulation of Investigatory Powers Act 2000

<http://www.hmso.gov.uk/acts/acts2000/20000023.htm>

It is an offence punishable with imprisonment of a term up to two years, a fine or a combination of both, to intercept communications without authorisation.

# Freedom of Information Act 2000

Creates the public right (with few exceptions)

- To be told if information is held by a public authority (including universities)
- To obtain information held by public authorities

# Records Management Tools 1

Typically

Manuals governing registration and filing

Security and confidentiality procedures

(guiding levels of sensitivity and who should have access to what)

Classification schemes (usually metadata reflecting hierarchy of use and intellectual content)

Records/digital assets surveys (establishing who has created what, for what purpose and what needs to be done about it for long term management)

Records Retention/Disposition Schedule (an organisation wide scheme guiding how long records should be kept by who and who should destroy )

Tool kits including a range of detailed guidance to reduce bulk or support preservation

Targeted microfilming/scanning

# Records Management Toolkit

- 1 How to find out which legislation affects your records
- 2 How to comply with the Data Protection Act 1998
- 3 How to comply with the Freedom of Information Act 2000
- 4 How to classify your records
- 5 How to manage your paper files
- 6 How to store your paper-based records
- 7 How to transfer your records from archives
- 8 How to request loans of your records from archives
- 9 How to destroy your records
- 10 How to keep your information securely
- 11 How to manage your e-mail
- 12 How to manage your electronic records
- 13 How to dispose of your records when you leave King's College London
- 14 How to manage electronic documents using Microsoft Office
- 15 How to manage academic research records
- 16 How to manage student records
- 17 How to manage personnel records [draft, not yet approved]
- 18 How to manage your records as a personal tutor

# Records Management Tools 2

Rarely:

Whole scale scanning. Media transfer and/or additional storage may solve storage problems but may exacerbate retrieval and add to burden and cost of answering Data Protection and FOI enquiries.

Large scale EDMS/ERMS schemes. In ambition they are often excellent but few universities have the degree of intellectual control required to implement them effectively. Used to address specific problems they may be helpful.

# USICA Members Survey 2004/5

## Priority concerns overall

- |          |                                      |
|----------|--------------------------------------|
| Number 2 | Strategic approach to infrastructure |
| 4        | Anytime, anywhere computing          |
| 7        | IT institutional policy              |

## Priority concerns over next 12 months

- |          |                     |
|----------|---------------------|
| Number 5 | User management     |
| 6        | Document management |

## Heads of IT Services

- |          |                                      |
|----------|--------------------------------------|
| Number 1 | Strategic approach to infrastructure |
| 6        | Determining priorities               |
| 8        | User management                      |
| 9        | Departmental relationships           |
| 10       | Customer centric services            |

# The Art of the Possible

Information Security Toolkit?

Life cycle management of information?

Full legal compliance?

# Progress at King's College London 1

- 2001      Records Disposition Schedule
- identified who had functional responsibility for content (not as obvious as you'd think)
  - identified key records series and defined appropriate retention/destruction periods for corporate records
- 2002      Records Management Policy. High level endorsement of need to manage
- 2003-4    Development of Records Management Toolkit, a how to manual which is growing. Several sections written in collaboration with IT (called IS at King's College)
- 2003-4    Surveys and training regularly offered

Broadly speaking we now know who has got what series of records or information and who is responsible for it and areas of concern

# Progress at King's College London 2

- 2004 Conducted JISC funded 'What is a student record?' Project to agree detail collegiately about what constituted core information on students
- 2004-5 Conducted JISC funded survey of digital assets to help focus on issues relating to preservation and develop a basis for joined up thinking on business continuity with respect to digital information
- 2005 Digital Assets Working Party established to prioritise findings and implement
- 2006 Survey of research assets planned. Regarded as intellectual capital asset and source of legal exposure under Data Protection but fell outside JISC survey

# Progress at King's College London 3

- 2004 Information Security Policy based on BS7799 approved by Council. Drafted by the Records Manager with input from IT. Risks to security threatened both business effectiveness and legal compliance
- 2004 Information Security Group established by IT to exchange local current awareness and best practice in response to threats
- 2005 Web Accessibility Policy approved by Council

# Progress at King's College London 4

- 2003-4 Extensive training offered on the information implications of the Data Protection and Freedom of Information Acts
- JISC draft Freedom of Information and Publication Schedule tested. Underlined the need for greater detail in the Records Disposition Schedule and need for a Web Content Management System to control creation and management of data that was likely to become public.
  - Freedom of Information Publication Schedule published

# Progress at King's College London 5

- 2005 Information Services & Systems Regulations (covering IT, library and archives, and including emails and web) fully revised, integrated and made coherently applicable to staff and students. The different elements had been previously developed at different times and provided loopholes for offenders as well as being out of date. All staff and students now notified.
- 2005 Freedom of Information & Data Protection Policies prepared for Council approved  
To ensure all staff knew what was expected
- 2005/6 Email policy. Draft under preparation. Although email is covered by much of the above the sheer scale and immediacy of e-mail required a specific focus

# Progress at King's College London 6

- 2005 Web Content Management System implemented  
FOI work revealed large quantities of out of date material and differing approaches to presenting information
- 2005 Email filtering contracted out
- Late  
2005 Business continuity planning software acquired. Population and high level buy-in needs work
- Late  
2005 Protocol on handling FOI requests reviewed and confirmed. Need for sustained work on records management both to speed up identification of detailed information sought and ensure the ordered destruction of drafts and other redundant data confirmed

# Conclusion

The successful implementation of both information security and records management requires

- Up to date knowledge of available technological solutions
- Sustained and vigorous monitoring of risk
- Extensive knowledge of the broad (and sometimes) detailed content of the information being protected
- A working knowledge of the law (which is struggling to keep up with technology)
- Rigorous prioritisation of both risk and content
- Partnership working within our organisations among different professions