RECORDS MANAGEMENT SYSTEMS
IT'S GOT TO BE IN THERE SOMEWHERE!
Rick

INSTITUTE OF ADVANCED LEGAL STUDIES | SCHOOL OF ADVANCED STUDY UNIVERSITY OF LONDON

THE LEGAL RECORDS AT RISK (LRAR) PROJECT

Project Patrons:
William Twining, Quain Professor of Jurisprudence Emeritus, UCL
Avrom Sherr, Emeritus Professor, IALS

Project Director: Clare.cowling@sas.ac.uk

http://ials.sas.ac.uk/research/areas-research/legal-records-risk-lrar-project

Cartoon reproduced courtesy of the National Archives of Australia

Legal Records at Risk Guideline 7: advice to legal institutions on digital continuity and managing digital records

Most information and data created or managed by institutions specialised to law are now born-digital. Existing technology does not, however, always provide adequate solutions to the challenges of digital working. We risk losing key information and corporate knowledge. Information is hard to find, and if it is found, may lack an "administrative history" – the context necessary to interpret it. It may exist in many formats and be duplicated many times and, after an astonishingly short space of time, it may become inaccessible through digital obsolescence.

Information compliance and records management requirements need to be included in all IT systems planning from the beginning, not added on as an afterthought or when a system nears obsolescence, when it may be too late to save valuable records. *This is a particular issue for client files, which may have to be accessible for decades*.

Where information and records management requirements are not clearly defined from the beginning systems quickly become overloaded, particularly if there are no automated disposal rules to allow deletion of documents and data. Some sort of bulk "archiving" action may then have to be taken by IT to reduce the storage problem. This "archived" information also needs to be subject to clear management and disposal rules, otherwise the costs of retaining all data indefinitely and unnecessarily (and, where personal data is involved, illegally in violation of Principle 5 of the Data Protection Act) – and of having to locate, retrieve, assess and produce it - will continue to spiral.

Disclosure and information risk

It should always be remembered that all surviving information (including data in backup tapes, databases, line of business systems, shared or personal drives and email) is potentially disclosable under the Data Protection Act (where there is personal data) or in connection with a litigation disclosure process.

Not managing information properly heightens risk and cost, especially around e-disclosure for litigation purposes.

There is also a risk that digital information will not be accepted in a UK court if it has not been managed in accordance with best practice standards like BS 10008:2014 Evidential Weight and Legal Admissibility of Electronic Information.

Disposing of digital records – deleting, purging and archiving

What is “Archiving”?

In the IT world archiving means the bulk removal of information and data to cheaper storage once it is either a) no longer needed for day to day work or b) the system in which it is stored becomes overloaded. This is a *temporary* solution to reduce storage costs. It does not solve the issue of how long to keep the information; if it is kept indefinitely the cost of storage, management and retrieval will spiral in exactly the same way as the costs of keeping paper records.

Archiving in the true, professional sense means the selection of (usually about 5%) of those records of an individual or organisation which have permanent research value and their deposit in an archive repository (either in-house or 3rd party) which will make them available for research once any sensitivity has expired. The remaining 95% of records can be destroyed once the organisation/ individual no longer needs them.

In the paper world such records were not deposited in an archive until their business use had expired. In the digital world this may not be possible as the records could well have disappeared or become inaccessible through digital obsolescence before they can be collected for deposit. Digital records are therefore more at risk than their paper counterparts.

This risk means that, where a legal organisation or practitioner knows that some digital records have permanent value as an asset, they should take steps to:

a) identify and tag them on creation or receipt;
b) ensure that the system and format in which they are stored will render them accessible over the long-term; and
c) arrange for the archives to take custody of them *before* they become inaccessible through system decommissioning or data migration.

How do we safely dispose of digital information? By *either* archiving *or* deletion

The regular disposal of digital information and data when no longer needed means that the fiscal, legal, operational and historic value of records has been identified (preferably on creation), that deletion or archiving rules have been put in place and that information risk and storage costs are consequently reduced.

Deleting obsolete digital information:

- All individuals within organisations are capable of – and should regularly delete - redundant material so that ephemeral data and documents are not stored unnecessarily (eg drafts, duplicates, inaccurate material, obsolete versions and old reference material).
- All organisations should maintain and implement regularly updated information retention and destruction schedules and instruct their IT departments on when to purge redundant material.
- The Archivist or Records/Information Manager should be involved in all planning for new, or decommissioning of old, IT systems and for any “archiving” by IT.

Archiving digital information

- For in-house archives the Archivist should have full access to IT systems to enable early selection of information of permanent value.
- Where an organisation has a deposit arrangement with a 3rd party archives the deposit agreement should specify:
  a) frequency of digital deposits (eg annually);
  b) method of deposit (eg secure file transfer protocol; encrypted USB or hard drive);
  c) format of deposits (eg PDF);
  d) closure periods and
  e) the arrangements the archives will make to ensure accessibility and digital continuity over time.