IALS 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

Legal Records at Risk Guideline 9: advice to legal institutions on managing documents in shared network drives

What are shared network drives?

- They are electronic storage areas on the network for corporate documents which we need to work on/share within a defined group. We usually group them into shared folders.
- We use shared folders to store what is known as "unstructured data" (eg Word documents, Excel spreadsheets, emails, PowerPoint, PDFs etc).
- Each business area or team is responsible for managing its own shared folders.

How has this created problems in the past?

- No rules or guidelines on creating or naming shared folders.
- Ownership of shared folders and sub-folders not clearly defined.

And the result has been...

- Duplication of information within and between folders (compliance/efficiency risk).
- No-one is sure which document in which folder is the correct/latest version (compliance/ reputational risk).
- Unauthorised access to information is a constant danger (compliance risk).
- No-one is sure when to delete obsolete, inaccurate or out-of-date information (compliance/ efficiency/financial risk).
- No-one takes responsibility for managing any of the above risks!

Setting up a new top level shared folder within a shared network drive:

- Each top level folder must have an assigned owner who is responsible for its content.
- Anyone wishing to set up a new top level shared folder should think carefully about whether the folder is needed or whether an existing folder will suffice.
- The person setting up the folder is responsible for managing both the folder and its contents in line with best practice, for ensuring other team members follow best practice when adding new content and for deleting the folder and its contents once it is no longer needed so that they no longer appear in the shared drive.
- All users of the folder, however, need to assume responsibility for managing the information they store in it: see overleaf.

What's the solution?

- Managing information risk is everyone's responsibility: see overleaf.

Managing folders	**Managing files/documents within folders**
Plan properly when setting up a folder: • One folder = one function. What is it designed to store? Case files? Complaints/enquiries? Project documents? Committee/team meetings? • Who needs to have access to it? • Have all users had input into/been warned about/shown the new structure? Take responsibility • The shared folder needs a designated owner. • The owner should regularly review the folder's content and purpose to see whether it is still current or no longer needed. • The owner should monitor any sub-folders which may be added to make sure they are relevant to the parent folder's purpose and are given meaningful titles. Keep it simple • Give folders meaningful titles (ie names everyone will understand), which reflect clearly what the folder is about. • Allow as few sub-folder layers as possible to speed access and reduce file-path length. • Store documents in the *most relevant folder* (ie the one covering the primary function to which the document relates). Dispose of obsolete information • Delete redundant material so that ephemeral documents are not stored unnecessarily (eg drafts, duplicates, obsolete versions and old reference material). • Folder owners should regularly review the folder contents to check that they are still being used or referenced. If not, the folder should be deleted; this will reduce clutter and speed retrieval of business critical documents. • The corporate retention schedule should be used to review and delete obsolete content. If there isn't a schedule, one needs to be created to reduce compliance risk and information overload.	Use accurate, meaningful titles • *Never* use an individual's name as a folder or file/document title (eg 'Fred's docs') – they don't reflect the folder's purpose and mean nothing to other colleagues. • Avoid repetition – the folder name will be in the file-path so there's no need to repeat it in the document eg: Committee\Committee meetings\Committee agenda.doc • Will there be several versions? If so, include the version number in the title (eg v1.0) • Will you need to browse by date? If so, *always* include the date at the beginning of the title as follows: **YYYY-MM-DD** (eg 2016-06-30). Documents will then be listed in the correct chronological order – invaluable for records of agenda and meetings. • Acronyms go out of date quickly – if you *must* use them keep a key to what they mean in, eg, an Administration folder. Avoid duplication • Don't file a document in more than one place. Use shortcuts to find it in other folders (right click on the document title, click 'create shortcut' and then move the shortcut to the relevant folder). • When e-mailing information to other users of the shared folder send hyperlinks to documents, not attachments. Don't forget about managing e-mail! • Business critical e-mails should be stored, like any other document, in the shared area. • If there is no document management system with email integration to automatically store emails you will have to move business critical e-mails out of your mailbox folders and into the relevant shared folder manually as soon as the transaction is complete. Tedious but necessary if the email needs to be accessed by others or kept as evidence.