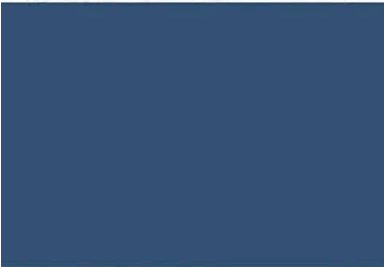


# RISK RULE

## Document Management



*If it's not written down, then it didn't happen.*

Although the law does not actually say this, it is a good principle for putting document management into perspective.

Courts and tribunals are skeptical about the accuracy of unaided human memory, and professional witnesses in particular are vulnerable to claims that their memory cannot be accurate over a long period where they might have worked on many similar projects. Cross-examining barristers may exploit a professional's tendency to remember what they *usually* did, rather than having a crystal clear memory of what they in fact did on the project in question.

Rely on memory alone at your peril. A witness whose memory is supported by contemporaneous written records (which means records created very close to the time that the event they describe took place) is more credible to the courts. Equally, a professional who can produce a good file with comprehensive written records gives an impression of thorough competence.

### What sort of records?

You need all the records that a prudent consultant would create. Design documents, certainly. Correspondence (letters, faxes, emails) with clients and other parties, minutes of meetings, research or information relevant to your design decisions (such as manufacturer's product information), your own notes, photographs or film, file notes recording the substance of conversations you had, your brief and any documents which amend the brief.

Traditionally, in the event of a claim, the courts would only accept original paper documents as evidence. These days, evidence legislation has broadened the rules. "Document" is now defined to include almost any record of information, and copies and electronic versions of documents may be used as evidence.

Remember that a court will attach greater weight to a document if its integrity and reliability can be established, especially when it comes to electronically stored information. For this reason, the successful defence of a claim against you may depend on the quality of the

document management systems in your practice and your ability to prove that they were regularly and reliably followed.

### A formal policy

Develop a written protocol for document management in relation to both hard copy documents and electronically stored information. Obviously the protocol will be as detailed and sophisticated as is appropriate to your scale of practice, but bear in mind that the importance of document management and the range of documents needed to defend claims is the same for small projects as for large ones.

The protocol should address the methods by which information is created, stored, reproduced, archived and destroyed. All staff need a copy of the protocol. The more diligently the protocol is followed, the easier it will be for you to track and retrieve records, and the more credible those records will be in the event of a dispute.

### What makes a good file note?

The purpose of a file note is to support your memory, so that if needed you can attest accurately to the event recorded in it. A good file note starts with the date and (if relevant) time, the name of the person taking the note, the other people present, and the name and number that identify the project. It gives a summary of the key points that were discussed, going into more detail on important issues. If handwritten, it needs to be legible, and signing it helps authenticate the note.

### Emails and electronic information

Emails relating to a project need to be readily accessed should a claim arise. Emails should either be printed and filed on a hard copy file, or electronically stored in a database specific to each project. Storing them merely in the email account of an individual staff member is not sufficient.

A clear written policy on sending, storing and archiving emails is important. Emails should not be regarded as a casual form of communication in a business environment. Anything said in an email is legally binding and can be used to defend or to attack you, so be especially vigilant about including damaging or reckless statements in an email, which can all too

easily be forwarded or copied to unintended recipients.

All of your electronic information needs to be backed up. Consider also drawing up a disaster recovery plan for accessing data and restoring your systems in the event of a complete failure.

Generally, hard copy records are preferable to electronic because they are not quite as susceptible to loss or damage. To store records only in electronic form, you need to be confident that you can retrieve them if they are needed to defend a claim against you, and that your electronic storage systems allow you to attest accurately to the origin, history and interpretation of the documents they contain. Remember that simple details, like the date on which a file note was created, can become crucial to a dispute.

If you update your IT systems, either upgrade all old files so that they are compatible with the new system, or retain a version of the old software and hardware so that the old files can be accessed if they are required.

On projects which are managed by means of an online project management system which is controlled by others, consider making it a condition of participation that you receive copies of all relevant information on the system either at regular intervals throughout the project or, at least, upon completion of your services. In any situation where editable electronic records leave your control, it is important to keep an exact copy of each document, so that any changes made by others can easily be traced.

### Archiving

A formal policy for document retention and destruction helps prevent misplacement and inadvertent destruction of documents, and counters allegations of unscrupulous disposal.

Retain all documents relevant to your work on a particular project. Spare copies can usually be discarded, so long as they are identical to the copy that you retain. Paper documents which are scanned and stored electronically (with the original being destroyed) can still be used as evidence, but the original paper copy is slightly better evidence. Keep the original where possible, especially if it contains important elements such as a handwritten signature.

When considering how long to retain your documents, take into account the fact that claims arising from construction projects often occur many months or even years after construction has been completed. Because the various limitation laws are not entirely comprehensive, there is still a possibility (albeit increasingly small) of claims being made against you ten, twenty or even fifty years after completion. The longer you retain your project documentation, the better the position you are likely to be in to defend any claims that arise. We recommend keeping your documents for at least ten years, and longer if possible.

Your general legal obligations (e.g. under tax-related laws) and any specific document management clauses in your consultancy agreement may also require you to

keep documents on a particular project for a specified period. If an unusual retention period applies, it needs to be clearly marked on the file when it goes into archives.

### Destruction

It is a contempt of court to destroy documents if they are relevant to legal proceedings which are underway. In some states, it is also a criminal offence to destroy documents which are relevant to foreseeable legal proceedings, even if those proceedings had not yet been commenced at the time the documents were destroyed. Because documents are vital evidence, the law punishes parties for destroying them with ulterior motives.

A good document destruction procedure prevents inadvertent destruction, and leaves a paper trail to prove that the destruction was merely routine, not malicious.

Any file destruction should first be authorised by a senior staff member, preferably the project leader. They should assess whether any disputes exist on the project, or are anticipated. In either of those cases, the file should be returned to archives with a new expiry date, upon which its destruction will be reconsidered.

If there are no existing or anticipated disputes on the project, then a document destruction checklist should be completed. (The document destruction policy should include a pro forma checklist.) The checklist should record, among other things, a description of the documents contained in the file, those matters considered before the file was destroyed (such as the prospect of litigation, and whether retention is required by law or by contract), the name of the person authorising destruction, and the date on which the file was destroyed. This checklist should be retained in a central register, for easy reference if the destruction is ever questioned.

Finally, consider whether the file needs thorough destruction rather than simply being placed in the bin, since it is likely to contain information which is confidential to your client.

Once these steps have been completed, the file can be put through the shredder.

(Also see our Risk Rule — Electronic Documents Checklist which contains specific suggestions with respect to storage and transfer of electronic documents.)