

Guide to Keeping Records in Digital Form Only

This guidance is based on the British Standard BS 10008:2008 and one of its supporting Codes of Practice BIP 0008-1 concerning information stored electronically.

The British Standards Institution issued a Code of Practice for Legal Admissibility of Information Stored on Electronic Document Management Systems, (BIP 0008 which was updated in 2014). This code of practice provides guidance to ensure, as far as possible, that electronic documents and scanned images will be accepted as evidence by the courts.

The key principles behind BIP 0008 are:

1. Authenticity – Processes to be followed at system planning, implementation and the procedures by which the systems should be operated.
2. Storage and access procedures – Procedures including scanning, indexing, retrieval, system administration, archiving, off-site storage and training, to be followed
3. Demonstrability of adherence – A structured audit process resulting in a Certificate of Conformity that displays demonstrability of adherence.

If keeping a record in digital form only, the following should be considered:

- The record must be able to be found in a timely manner and opened in a readable form.
- It must be proved that the contents of a data file existing within an electronic management system has not changed since the time of storage. If required for legal reasons this will prove the absolute authenticity of electronically stored documents and will be crucial to their admissibility. Therefore if a document arrives in an email, this should be stored in an appropriate area with the document still attached. If scanned, dates, page numbers and signatures should be clearly visible.
- Where a document is scanned and the original destroyed, records must be kept on the system i.e. an audit trail of key information. This establishes that the original paper copies are destroyed and that, as a result, the scanned images are deemed to be the originals. All retention and destruction procedures must be recorded. Certificates of destruction are available from Estates Records Management.
- Originals should not be destroyed until it is clear that processes have been completed properly. The audit trail, as a minimum, should log details of each significant event relevant to the document in the system. It should be automated, contain relevant data such as date/time for every change/access, be unalterable, stored in accordance with the information management policy, and be backed-up.
- The absence of any one of these attributes would render the information effectively lost within the system and not fit for purpose or meaning.