Destruction and Retention Policy

Information held for longer than is necessary carries additional risk and cost. Records and information should only be retained for legitimate business use. Under the Data Protection Act 1998, personal data processed by LEASE must not be retained for longer than is necessary for its lawful purpose.

When records are no longer required by LEASE and do not have historic value (see below) they should be destroyed.

The default standard retention period for LEASE records is 7 years plus current, otherwise known as 7 years + 1. This is defined as 7 years after the last entry in a record, followed by first review and/or destruction to be carried out in the additional current (+ 1) year.

Records must only be retained beyond the default LEASE retention period if their retention can be justified for statutory, regulatory, legal or security reasons or for their historic value.

Historic value documents

Historic value is about value for corporate memory purposes. The kinds of records that have historic value are:

- records documenting the origins and legal status of the organisation - eg Memorandum & Articles of Association
- records providing evidence of the organisation's structure, policies and key decisions eg Board minutes
- records documenting the obligations, rights and entitlements of the organisation and those with whom it deals, including evidence of compliance with regulations and procedures -
- key publications produced by the organisation, including information published on the website (unless these survive elsewhere)
- information that provides significant context and background to the archives, e.g. organisation charts, historical narratives and selected public relations material

We also need to be able to explain the absence of records that were once held. For this reason, it is recommended that disposal decisions are clearly documented.

Essentially, destruction documentation should provide evidence that the destruction took place in accordance with established and formally adopted policies and schedules and with appropriate authorisation. Without this it may be difficult to demonstrate that records were not eliminated to avoid disclosing them in response to a request for information.

Accordingly, Disposal Schedules are created and maintained in a database. It is useful to have schedules which show what disposal decisions have been made, on what basis and that they were duly authorised. Therefore, a hardcopy should also be printed out and retained. An example follows:

Identifier (short title/ description	Reason for disposal decision	Confidentiality/ security/ personal data issues	Notes	Approved for destruction by	Date of destruction	Destruction method

Once a disposal schedule has been drafted, it needs to be agreed and authorised. It should then be approved by senior management. The details from the approved schedule should be copied into the database.

All records should be destroyed with the level of security required by the confidentiality of their contents. So, for example, if records containing sensitive personal data or protectively marked papers have been shredded, the shredded paper should be handled securely, not dumped. And, of course, records awaiting destruction should be stored securely.