5. Storage and maintenance of records

Knowing what records are held

5.1 The effectiveness of records systems depends on knowledge of what records are held, what information they contain, in what form they are made accessible, what value they have to the organisation and how they relate to organisational functions. Without this knowledge an authority will find it difficult to:

a) Locate and retrieve information required for business purposes or to respond to an information request;

b) Produce a Publication Scheme[10] or a reliable list of information assets available for re-use;

c) Apply the controls required to manage risks associated with the records;

d) Ensure records are disposed of when no longer needed.

5.2 Authorities should gather and maintain data on records and information assets. This can be done in various ways, for example through surveys or audits of the records and information held by the authority. It should be held in an accessible format and should be kept up to date.

5.3 Authorities should consider publishing details of the types of records they hold to help members of the public planning to make a request for information under FOISA.

Storing records

5.4 Storage should provide protection to the level required by the nature, contents and value of the information in them. Records and information will vary in their strategic and operational value to the authority, and in their residual value for historical research, and storage and preservation arrangements reflecting their value should be put in place.

5.5 Authorities should be aware of any specific requirements for records storage that apply to them. For example, BS 5454:2000 makes recommendations for the storage and exhibition of archival documents, mainly those on paper and parchment.

5.6 Storage should follow accepted standards in respect of the storage environment, fire precautions, health and safety and, if applicable, physical organisation. It should allow easy and efficient retrieval of information but also minimise the risk of damage, loss or unauthorised access.

5.7 Records that are no longer required for frequent reference can be removed from current systems to off-line or near off-line (for digital media) or to off-site (for paper) storage where this is a more economical and efficient way to store them. They should continue to be subject to normal records management controls and procedures. The accessibility of these records should not be compromised.

5.8 The whereabouts of records should be known at all times and movement of files and other physical records between storage areas and office areas should be logged.

Ensuring records remain usable

5.9 Records should remain usable for as long as they are required. This means that it should continue to be possible to retrieve, use and rely on them.

5.10 Records in digital systems will not remain usable unless actions are taken. Authorities should put in place a strategy for their continued maintenance designed to ensure that information remains intact, reliable and usable for as long as it is required. The strategy should provide at a minimum for updating of the storage media and migration of the software format within which the information and metadata are held, and for regular monitoring of integrity and usability.

5.11 Records in digital systems are particularly vulnerable to accidental or unauthorised alteration, copying, movement or deletion which can happen without trace. This puts at risk the reliability of the records which could damage the authority's interests. Authorities should assess these risks and put appropriate safeguards in place.

5.12 Back-up copies of records in digital systems should be kept and stored securely in a separate location. They should be checked regularly to ensure that the storage medium has not degraded and the information remains intact and capable of being restored to operational use. Back-ups should be managed in a way that enables disposal decisions to be applied securely without compromising the authority's capacity to recover from system failures and major disasters.

5.13 Physical records such as paper files may also require regular monitoring. For example, formats such as early photocopies may be at risk of fading, and regular checks should be made of any information in such formats that is of continuing value to the authority.

5.14 Metadata for records in any format should be kept in such a way that it remains reliable and accessible for as long as it is required, which will be at least for the life of the records.

Business continuity plans

5.15 Business continuity plans should identify and safeguard records considered vital to the organisation, that is:

a) Records that would be essential to the continued functioning or reconstitution of the organisation in the event of a disaster;

b) Records that are essential to ongoing protection of the organisation's legal and financial rights.

The plans should include actions to protect and recover these records in particular.

Authorities should know what records they hold and where they are, and should ensure that they remain usable for as long as they are required.