6. Security and access

6.1 Authorities should ensure that their storage arrangements, handling procedures and arrangements for transmission of records reflect accepted standards and good practice in information security. It is good practice to have an information security policy addressing these points.

6.2 Ease of internal access will depend on the nature and sensitivity of the records. Access restrictions should be applied when necessary to protect the information concerned and should be kept up to date. Particular care should be taken with personal information about living individuals in order to comply with the 7th data protection principle, which requires precautions against unauthorised or unlawful processing, damage, loss or destruction. Within central Government, particular care should be taken with information bearing a protective marking. Other information, such as information obtained on a confidential basis, may also require particular protection.

6.3 Transmission of records, especially outside the authority's premises, should require authorisation. The method of transmission should be subject to risk assessment before a decision is made.

6.4 External access should be provided in accordance with relevant legislation.
6.5 An audit trail should be kept of provision of access, especially to people outside the immediate work area.

Authorities should ensure that records are stored securely and that access to them is controlled.