

7. Disposal of records

7.1 For the purpose of this Code, disposal means the decision as to whether the record should be destroyed or transferred to an archives service for permanent preservation, and the putting into effect of that decision.

General principle

7.2 As a general principle, records should be kept for as long as they are needed by the authority: for reference or accountability purposes, to comply with regulatory requirements or to protect legal and other rights and interests. Destruction at the end of this period ensures that office and server space are not used and costs are not incurred in maintaining records that are no longer required. For records containing personal information it also ensures compliance with the fifth data protection principle.

7.3 Records should not be kept after they have ceased to be of use to the authority unless:

They are known to be the subject of litigation or a request for information. If so, destruction should be delayed until the litigation is complete or, in the case of a request for information, all relevant complaint and appeal provisions have been exhausted;

They have long-term value for historical or other research and have been or should be selected for permanent preservation. (Note that records containing personal information can be kept indefinitely for historical research purposes because they thereby become exempt from the 5th data protection principle.)

They contain or relate to information recently released in response to a request under FOISA. This may indicate historical value and destruction should be delayed while this is re-assessed.

Making disposal decisions

7.4 Disposal of records should be undertaken only in accordance with clearly established policies that:

Reflect the authority's continuing need for access to the information or the potential value of the records for historical or other research;

Are based on consultation between records management staff, staff of the relevant business unit and, where appropriate, others such as legal advisers, archivists or external experts;

Authorities should define how long they need to keep particular records, should dispose of them when they are no longer needed and should be able to explain why records are no longer held.

Have been formally adopted by the authority;

Are applied by properly authorised staff;

Take account of security and confidentiality needs.

7.5 The policies should take the form of:

An overall policy, stating in broad terms the types of records likely to be selected for permanent preservation. The policy could be a separate policy, part of the records management policy or a preamble to a disposal schedule;

Disposal schedules which identify and describe records to which a pre-defined disposal action can be applied, for example destroy x years after [trigger event]; review after y years, transfer to archives for permanent preservation after z years.

7.6 Disposal schedules should contain sufficient details about the records to enable the records to be easily identified and the disposal action applied to them on a routine and timely basis. The amount of detail in disposal schedules will depend on the authority's needs but they should at least:

Describe the records, including any relevant reference numbers;

Identify the function to which the records relate and the business unit for that function (if that is not clear);

Specify the retention period, i.e. how long they are to be kept;

Specify what is to happen to them at the end of that period, i.e. the disposal action;

Note the legal, regulatory or other reason for the disposal period and action, for example a statutory provision.

7.7 Disposal schedules should be arranged in the way that best meets the authority's needs.

7.8 Disposal schedules should be kept up to date and should be amended if a relevant statutory provision changes. However, authorities should consider keeping information about previous provisions so that the basis on which records were previously destroyed can be explained.

7.9 If any records are not included in disposal schedules, special arrangements should be made to review them and decide whether they can be destroyed or should be selected for permanent preservation. Decisions of this nature should be documented and kept to provide evidence of which records have been identified for destruction, when the decision was made, and the reasons for the decision, where this is not apparent from the overall policy.

Implementing disposal decisions

7.10 Disposal schedules and disposal decisions should be implemented by properly authorised staff. Implementation arrangements should take account of variations caused by, for example, outstanding requests for information or litigation.

7.11 Records scheduled for destruction should be destroyed in as secure a manner as required by the level of confidentiality or security markings they bear. For example, records containing personal information about living individuals should be destroyed in a way that prevents unauthorised access (this is required to comply with the 7th data protection principle). With digital records it may be necessary to do more than overwrite the data to ensure the information is destroyed.

7.12 When destruction is carried out by an external contractor, the contract should stipulate that the security and access arrangements established for the records will continue to be applied until destruction has taken place.

7.13 In some cases there will be more than one copy of a record. For example, there are likely to be back-up copies of digital records, or there may be digital copies of paper records. A record cannot be considered to have been completely destroyed until all copies, including back-up copies, have been destroyed, if there is a possibility that the data could be recovered.

Documenting the destruction of records

7.14 Details of destruction of records should be kept, either as part of the audit trail metadata or separately. Ideally, some evidence of destruction should be kept indefinitely because the previous existence of records may be relevant information. However, the level of detail and for how long it should be kept will depend on an assessment of the costs and the risks to the authority if detailed information cannot be produced on request.

7.15 At the very least it should be possible to provide evidence that as part of routine records management processes destruction of a specified type of record of a specified age range took place in accordance with a specified provision of the disposal schedule. Evidence of this nature will enable an authority and its staff to explain why records specified in a court order cannot be provided or to defend themselves against a charge under section 65 of FOISA that records were destroyed in order to prevent their disclosure in response to a request for information.