

# **Complying with the Records Management Code: Evaluation Workbook and Methodology**

**Module 2: Record Management policy statement**

## Module 2: Record Management policy statement

### General

- 4.1 This module deals with the need to establish a records management policy supported and mandated by senior management across the whole organisation and provides the module to undertake such an assessment. The policy should be comprehensive and cover all activities falling within the records management function. There should be a mechanism for regular review of the policy's relevance.
- 4.2 The relevant workbook questions which should be used to assess whether an organisation's record management policy or policies comply with the Records Management Code and supporting best practice guidance commence on page 5.

### Context and objectives

- 4.3 The Records Management Code states that:

*An authority should have in place an overall policy statement, endorsed by top management and made readily available to staff at all levels of the organisation, on how it manages its records, including electronic records.*

*This policy statement should provide a mandate for the performance of all records and information management functions. In particular, it should set out an authority's commitment to create, keep and manage records which document its principal activities. The policy should also outline the role of records management and its relationship to the authority's overall strategy; define roles and responsibilities including the responsibility of individuals to document their actions and decisions in the authority's records, and to dispose of records; provide a framework for supporting standards, procedures and guidelines; and indicate the way in which compliance with the policy and its supporting standards, procedures and guidelines will be monitored.*

*The policy statement should be reviewed at regular intervals (at least once every three years) and, if appropriate, amended to maintain its relevance*

- 4.4 The Lord Chancellors' Code extends these principles to the management of electronic or digital records. Specifically it states that:

*The principal issues for the management of electronic records are the same as those for the management of any record. They include, for example the creation of authentic records, the tracking of records and disposal arrangements. However, the means by which these issues are addressed in the electronic environment will be different.*

*Effective electronic record keeping requires:*

- *a clear understanding of the nature of electronic records;*
- *the creation of records and metadata necessary to document business processes: this should be part of the systems which hold the records;*
- *the maintenance of a structure of folders to reflect logical groupings of records;*
- *the secure maintenance of the integrity of electronic records;*
- *the accessibility and use of electronic records for as long as required (which may include their migration across systems);*
- *the application of appropriate disposal procedures, including procedures for archiving; and*
- *the ability to cross reference electronic records to their paper counterparts in a mixed environment.*

4.5 A formally agreed records management policy is essential for directing how records will be managed in a public authority. The policy establishes how records are created, captured, maintained and disposed of in accordance with the legal, regulatory and business needs of the public authority. It informs everyone of the place of records management in the organisation, both strategically and operationally.

4.6 In this context a policy may consist of one document or a series of documents which taken together provide a comprehensive records management policy. Whilst it is preferable to have one distinct policy and references to it in other linked policy documents some organisations' may have conflated records management into other policies for example information management or information security policies. A records management policy may be a records management specific policy document or it may emerge from policies for other organisational business activities, which set out rules for recordkeeping. However whatever the preferred mechanism or form for developing or incorporating the policy within an organisation records management must be directed by policy adopted at the corporate level and should be transparent to the reader.

4.7 The policy must direct that records are made, captured, maintained and disposed of in accordance with the legal, regulatory and business needs of the public authority and define the responsibilities of the personnel who manage records or carry out recordkeeping activities.

4.8 Many organisations may have a separate e-mail management policy, which augments the record management policy.

## Relevant guidance

- 4.9 Each sector may have its own sector specific rules, regulations and guidance and readers of this workbook should reference such guidance when establishing a record keeping or management system. Additional guidance on this subject has been provided by The National Archives (TNA) and is available on the TNA web-site. They include:

*Guidelines for management, appraisal and preservation of electronic records: Volume 1 Principles*

This guidance document sets out the principles of electronic records management and outlines broad strategies for translating the principles into practice. It can be accessed at the following web address:

<http://www.nationalarchives.gov.uk/electronicrecords/advice/guidelines.htm>

Other directly relevant publications include:

*Corporate Policy on Electronic Records*

*Guidelines on Developing a Policy on Managing e-mail*

*Managing Web Resources: Management of Electronic Records on Web-Sites and Intranets: An ERM Toolkit*

These are available at the TNA web-site at:

<http://www.nationalarchives.gov.uk/electronicrecords/advice/>

## Evaluation questionnaire

- 4.10 The records management policy statement will provide a mandate for the performance of all records and information management functions and the final records management policy statement having secured its approval by senior management should be made available to all staff.
- 4.11 To assess whether the required elements are in place the questions in the table which follows, numbered 1 to 46 in this workbook, have been provided to elicit whether the information required for an appropriately compliant assessment is actually explicitly addressed in the organisation's record management policy or its equivalent where records management policy has been subsumed within other official policy documents. Guidance on how to analyse the responses to these questions is provided in the chapter entitled *Risk evaluation and development of mitigation strategies*.

1. *Is there a policy statement on how the organisation manages its records?* Yes  No  N/A

Reference

---

2. *Does the policy explicitly include records in electronic or digital form as well physical form (e.g. paper or microform)?* Yes  No  N/A

Reference

---

3. *Does the policy make explicit that e-mails produced or received in the conduct of business are considered to be part of the corporate record?* Yes  No  N/A

Reference

---

4. *Does the policy fully reflect the statutory and regulatory environment within which the organisation is required to operate?* Yes  No  N/A

Reference

---

5. *Is the policy formally endorsed by senior management within the organisation?* Yes  No  N/A

Reference

---

6. *Does the policy define roles and responsibilities to support the record management function?* Yes  No  N/A

Reference

---

7. *Does the policy define the responsibility of individuals to document their actions and decisions in the organisation's records?* Yes  No  N/A

Reference

---

8. Does the policy define criteria for disposing of obsolete records? Yes  No  N/A

Reference

---

9. Has responsibility for identifying and disposing of obsolete records in an auditable manner been assigned to a role(s)? Yes  No  N/A

Reference

---

10. Does the policy provide a framework for supporting appropriate standards, procedures and guidelines? Yes  No  N/A

Reference

---

11. Is the policy readily available to all staff at all levels of the organisation? Yes  No  N/A

Reference

---

12. Are newly appointed personnel (including temporary staff and consultants) made formally aware of the policy? Yes  No  N/A

Reference

---

13. Does the policy clearly indicate its place within the strategic and policy framework of the organisation and refer to data protection, freedom of information and information security policies? Yes  No  N/A

Reference

---

14. Does the policy define the requirements that must be met for the records themselves to be considered as a proper record of the activity of the organisation? Yes  No  N/A

*For example possible elements that might be identified for inclusion are:*

- a. the type of information transactions or communications which should be captured by the business*
- b. the preferred physical or logical form of the record*
- c. the location to be used by each part of the business in a classification system or file-plan*
- d. key metadata attributes (e.g. author, owner, nature of the record – contract, invoice, minutes FOI enquiry etc)*

Reference

---

15. Does the policy require that all systems and processes that deal with records incorporate measures to ensure the quality and reliability of the records, which must be maintained to provide a valuable information and knowledge resource for the whole organisation? Yes  No  N/A

Reference

---

16. Does the policy provide for an implementation plan across the organisation? Yes  No  N/A

Reference

---

17. Does the policy include provision for a technical policy to establish the criteria that can be applied to new types of technologies that process electronic records? Yes  No  N/A

Reference

---

18. Does the policy include provisions for a preservation or maintenance policy to ensure that electronic records are visibly present and maintained in an authentic state for as long as they continue to be required? Yes  No  N/A

Reference

---

19. Does the policy include provision for the preservation and secure storage of physical records for as long as they continue to be required? Yes  No  N/A

Reference

---

20. Does the policy establish a priority for the allocation of the resources needed to preserve the records intact for as long as they continue to be required? Yes  No  N/A

Reference

---

21. Does the policy make provision for the registration of its records in conformance with BS ISO 15489 (Information and Documentation - Records Management Standard)? Yes  No  N/A

Reference

---

22. *In accordance with BS ISO 15489 does the policy require that electronic records should be classified into a business classification scheme or file-plan developed for the organisation to ensure an integrated information structure across the organisation?* Yes  No  N/A

Reference

---

23. *Does the policy require that where records in physical form (i.e. paper records) are to be retained that they should be stored in physical folders, which are referenced and retrieved in accordance with references, displayed within the business classification scheme?* Yes  No  N/A

*(Note: some organisations may use formal registered files which display agreed titles and/or reference codes/numbers for this purpose)*

Reference

---

24. *Does the policy require that electronic records stored within a business classification scheme should each be provided with a unique title in accordance with a agreed naming policies or taxonomies adopted by the organisation to ensure accurate retrieval?* Yes  No  N/A

Reference

---

25. *Does the policy require that audits be undertaken of the registration and classification references used by the organisation so that the system makes sense and relevant records can be found in appropriate search sequences?* Yes  No  N/A

Reference

---

26. *Does the policy require that where relationships exist between different sets of records and different types of records (e.g. electronic and paper) these relationships are documented by the allocation of meaningful references to ensure these links are readily apparent when undertaking appropriate search sequences?* Yes  No  N/A

Reference

---

27. Does the policy reference existing information security policy and procedures? Yes  No  N/A

Reference

---

28. Does the policy make provision for the establishment of roles or bodies within the organisation, which will be able to make an accurate judgement on the sensitivity of records to identify any restrictions and determine the groups or individuals within the organisation who should have access? Yes  No  N/A

Reference

---

29. Does the policy establish how extraordinary access requests to the records by personnel within the organisation are to be authorised and managed? Yes  No  N/A

*(Note: this question is concerned with the access regime for all personnel where there is a need to provide additional extraordinary access rights to an individual as opposed to those access rights an individual might possess via the role they are assigned to by the employing organisation.)*

Reference

---

30. Does the policy establish the principles by which access to the records or the information they contain may be granted in response to requests external to the organisation? Yes  No  N/A

Reference

---

31. Does the policy also clarify the links between the records management policy and existing data protection and freedom of information disclosure policies maintained by the organisation? Yes  No  N/A

Reference

---

32. Does the policy provide for the documentation of the reasons why records were released or withheld (including partial disclosure where information within the record or record series was masked or concealed) in response to requests for information under the Freedom of Information Act 2000; the Data Protection Act 1998 and the Environmental Information Regulations 2004(EIR)? Yes  No  N/A

Reference

---

33. Does the policy require that all reasonable steps be undertaken to ensure that the electronic records and processes dealing with them are secure and that the electronic records are safeguarded from alteration, misinterpretation or loss? Yes  No  N/A

Reference

---

34. Does the policy provide for the auditing of compliance with the policy and associated procedures and guidance? Yes  No  N/A

Reference

---

35. Does the policy provide for the concept of a trusted custodian to hold or be responsible for the management of inactive records (for records in electronic and physical form)? Yes  No  N/A

Reference

---

36. Does the policy provide for the development and implementation of disposal schedules and mechanisms to ensure records can be appropriately disposed of (including to an archives facility) in an accountable manner when they are no longer required? Yes  No  N/A

(Note: in many cases disposal equates to authorised destruction as the records are no longer required but the term disposal also extends to other actions which include identifying review dates where a future destruction date can be determined and transfer and export to other designated organisations including transfer to specialist archives for permanent preservation of selected records)

Reference

---

37. *Does the policy require that business continuity plans be amended to include provisions for the maintenance of records and record management processes to ensure a constant service is maintained in spite of any technical or strategic hitches that may occur?* Yes  No  N/A

Reference

---

38. *Does the policy make provision for the creation of back-ups to a corporately agreed standard to include updates for new electronic records and metadata?* Yes  No  N/A

Reference

---

39. *Does the policy require that a robust back-up restoration regime be established to restore back-ups should they be required?* Yes  No  N/A

Reference

---

40. *In the event backed-up data is required to be restored onto a live system does the policy make provision for the removal from the back up copies of any records which were formally destroyed or transferred from the live system, in accordance with an authorised procedure, after the back up was created?* Yes  No  N/A

*(Note: - this is to ensure conformance with FOI and Data Protection requirements)*

Reference

---

41. *Does the policy make provision for a disaster recovery plan in the event that electronic systems are compromised or physical records damaged?* Yes  No  N/A

Reference

---

42. Does the policy define the principles to identify vital and/or emergency records in the event of a catastrophic event occurring? Yes  No  N/A

Reference

---

43. Does the policy require for the policy and the implementation plan to be regularly reviewed and assign responsibility for this? Yes  No  N/A

Reference

---

44. Does the policy set criteria for the conduct of a review of the records management policy and its implementation? Yes  No  N/A

(Note: - this review should include any supporting standards, procedures and guidelines)

Reference

---

45. Has the responsibility for conducting periodic reviews of the policy been clearly assigned? Yes  No  N/A

Reference

---

46. Does the policy include provision for preparation of a periodic report to ascertain the continuing relevance and efficacy of the policy and for its submission to senior management for review? Yes  No  N/A

(Note periodic review of policies to confirm relevance is good practice – the organisation needs to determine the frequency for such a review to be undertaken and ideally this requirement should be incorporated within the policy)

Reference

---