Records Management Policy

Document Owner's Name	**Elizabeth Barber – Records Manager** **Tel: 03000 415812** **elizabeth.barber@kent.gov.uk**
Approved	

Contents

The footnotes in this document relate to compliance with the Lord Chancellor's Code of Practice on the management of records issued under section 46 of the Freedom of Information Act 2000.

1. Introduction

Effective data, information and records management:

- is at the core of every service provided by Kent County Council (KCC) whether directly to the people of Kent or as an internal support service[1].

- supports the implementation of the strategies outlined in Increasing Opportunities, Improving Outcomes: Kent County Council's Strategic Statement 2015 – 2020 and ensures that KCC creates data, information and records which are accurate, reliable and accessible.

- ensures that KCC can meet government requirements for open data and transparency.

2. Policy Objectives

The objective of this policy is to define a framework for KCC to manage data, information and records in compliance with its Constitution and the statutory framework in which it is required to operate.[2]

This policy contains overarching requirements to ensure that KCC:

- creates and manages accurate, authentic, reliable and accessible data, information and records to meet the authority's business needs;
- identifies data, information and records which should be disposed of and disposes of it in line with KCC's information security requirements;
- includes all business critical data, information and records in business continuity plans;
- can identify information which could be published as part of the Open Data and Transparency programme.

This policy identifies the requirements to bring about these outcomes but does not include any information about how to fulfil the requirements. The Information Management Manual contains all the information members of staff will require to implement this policy.

3. Scope

KCC is committed to creating, keeping and managing data, information and records which document its principal activities [3].

---

[1] The policy must outline the role of data, information and records management and its relationship to the authority's overall business strategy: Section 46 Workbook Q41

[2] The policy must fully reflect the statutory and regulatory environment within which the organisation is required to operate : Section 46 Workbook Q43

[3] The policy must set out the authority's commitment to create, keep and manage data, information and records which document its principal activities: Section 46 Workbook Q42

This policy covers data, information and records regardless of the media in which it is stored (i.e. physical or digital formats - including e-mails) which are deemed to be part of the corporate record[4].

This policy covers all data, information and records created by KCC including those created by contractors and partners working on KCC's behalf regardless of where they are created, stored or managed[5].

4. Roles and Responsibilities

All KCC employees are responsible for creating and maintaining data, information and records in relation to their work that are authentic and reliable.

It is the responsibility of each Service Unit to identify staff with specific responsibilities for information management in the Service Unit and these responsibilities should be defined in their job descriptions.[6]

The Head of Governance, Law and Democracy is the Data Protection Officer.

The Director of Strategy, Policy, Relationships and Corporate Assurance is the Senior Information Risk Owner (SIRO). The SIRO is responsible for ensuring that the appropriate resources are available to implement and monitor the Records Management Policy.

The head of each directorate is the Information Asset Owner for their directorate.

The Information Resilience and Transparency Team will be responsible for providing advice, policies, protocols and procedures to assist operational units to achieve compliance with all Information Governance legislation, data, information and records management practices.

The Records Manager is responsible for maintaining the information asset register, the information risk register and the retention schedule[7].

The Head of Libraries Registration and Archives is responsible for managing the day to day running of the Records Management Service. However, the Records Manager

[4] The policy must explicitly include data, information and records in electronic or digital form as well physical form (e.g. paper or microform): Section 46 Workbook Q46 and the policy must make explicit that e-mails and any other form of electronic correspondence used by the organisation which are produced or received in the conduct of business will be considered to be part of the corporate record: Section 46 Workbook Q47

[5] The policy must provide for the continuous, unambiguous ownership of its data, information and records stored, managed or hosted elsewhere: Section 46 Workbook Q44

[6] The policy must define the responsibility of individuals to document their actions and decisions in the organisation's data, information and records: Section 46 Workbook Q49

[7] The policy must mandate the establishment of a dedicated team to support the role of Data, information and records and Information Manager to carry out the record management roles and duties identified in the data, information and records management policy: Section 46 Workbook Q58

is responsible for ensuring that the Records Management Service remains compliant with current record keeping practices[8].

5. Record Creation and Storage

[See sections 7-8 of the Information Management Manual]

All KCC staff are responsible for creating and maintaining data, information and records[9] in relation to their work and storing them in a way that ensures they can be identified and retrieved[10] when required[11] using the methods laid out in the Information Management Manual[12].

Individual directorates must provide for the preservation and secure storage of all data, information and records regardless of the format in which they are stored in until they can be safely disposed of [13]. Records storage space in occupied office buildings must meet the specification laid down in the Information Management Manual. Principal copies of semi-current records should, where there is no available office space, be transferred to the Records Management Service until they have reached the end of their statutory retention period.

The Records Manager is the trusted custodian who is responsible for the management of inactive data, information and records held in physical format where the information asset owner can not be identified.[14]

---

[8] The policy must define roles and responsibilities to support the data, information and records management function: Section 46 Workbook Q48

[9] The policy must provide a view on the creation of duplicate copies generally and in what circumstances may these be permitted: Section 46 Workbook Q78

[10] The policy must 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: Section 46 Workbook Q68 and the policy must make provision for the establishment of a registration or classification policy for the management of its data, information and records Section 46 Workbook Q63

[11] The policy must require that where data, information and records in physical form (i.e. paper data, information and records) are to be retained that they should be stored in a manner which ensures they can be reliably identified and retrieved to satisfy continuing business needs: Section 46 Workbook Q65

[12]The policy must require that electronic records stored or referenced within a business classification scheme should each be provided with a unique title in accordance with agreed naming policies or taxonomies adopted by the organisation to ensure accurate classification and retrieval: Section 46 Workbook Q66 and the policy must require that electronic records should be registered, classified or indexed as a means of providing an appropriate level of context to provide an integrated information structure to support access and retrieval according to the business need: Section 46 Workbook Q64 and [12] The policy must 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: Section 46 Workbook Q73

[13] The policy must indicate the need to provide for the preservation and secure storage of physical data, information and records (e.g. paper files) for as long as they continue to be required: Section 46 Workbook Q61

[14] The policy must provide for the concept of a trusted custodian to hold or be responsible for the management of inactive data, information and records for data, information and records in electronic and physical form. Section 46 Workbook Q75

6. Information Communication Technology

This policy links to the appropriate technical policies which establish the criteria applied to electronic systems which process and store records.[15]

7. Digital Continuity

[See Specialist Guidance 5 in the Information Management Manual]

It is the responsibility of each Directorate to ensure that all digital data, information and records which must be kept for longer than 7 years meet the requirements of the Digital Continuity policy[16] and that the relevant resources provided to do this[17].

The Records Manager is the trusted custodian who is responsible for the management of inactive data, information and records held in electronic format where the information asset owner can not be identified.[18]

8. Record Retention and Disposal

[See section 9 of the Information Management Manual]

All data, information and records (regardless of the media in which they are stored) must be retained for the period of time identified in the corporate retention schedule[19]. The retention periods listed in the schedule are the minimum length of time which the data, information and records must be kept. Where necessary data, information and records may be kept for longer periods of time.

It is the responsibility of each directorate to identify those members of staff who are responsible for identifying and disposing of obsolete data, information and records in an auditable manner[20]. The disposal of all data, information and records must follow the requirements outlined in section 9.4 of the Information Management Manual [21].

---

[15]The policy must make provision for or links to a technical policy to establish the criteria that can be applied to new types of technologies that process electronic records: Section 46 Workbook Q59

[16] The policy must include provision for the definition of a preservation or maintenance strategy to ensure that electronic records are visibly present and maintained in an authentic state for as long as they continue to be required regardless of any technology change that may occur. Section 46 Workbook Q60

[17] The policy must establish a priority for the allocation of the resources needed to preserve electronic records intact for as long as they continue to be required. Section 46 Workbook Q62

[18] The policy must provide for the concept of a trusted custodian to hold or be responsible for the management of inactive data, information and records for data, information and records in electronic and physical form. Section 46 Workbook Q75

[19] The policy must define high level criteria for disposing of data, information and records no longer required for business purposes Section 46 Workbook Q50

[20] The policy must assign responsibility for identifying and disposing of obsolete data, information and records in an auditable manner to a role(s)Section 46 Workbook Q51

[21] The policy must provide for the development and implementation of authorised disposal procedures and mechanisms to ensure data, information and records can be appropriately disposed of (including to an historical archive institution) in an accountable manner when they are no longer required: Section 46 Workbook Q76

9. Access

Information Governance will be governed by the following policies:

- Freedom of Information policy[22]
- Data Protection policy
- Environmental Information Regulations Policy
- Open Data Policy
- Information Security Incident Policy and Protocol[23]
- Data Breach Policy

ICT will assign access permissions to individual members of staff on the request of individual line managers[24].

10. Business Continuity

Individual service units are responsible for identifying the data, information and records (regardless of the media in which they are stored) which are considered to be business critical and to ensure that the business critical elements are included in individual service unit business continuity plans[25]

Individual service units are also responsible for specifying operating parameters (extent and frequency) of the back up copies taken of the data, information and records such that they are fit for purpose.

It is the responsibility of ICT to ensure that backups are created to the agreed standards and to establish an effective back-up restoration regime to ensure that when back-ups need to be restored they remain fit for purpose[26].

---

[22] The policy must establish the principles by which access to the data, information and records or the information they contain may be granted in response to requests external to the organisation: Section 46 Workbook Q71 and the policy must 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; United Kingdom General Data Protection Regulation and the Environmental Information Regulations 2004(EIR): Section 46 Workbook Q72

[23]The policy must, or a clearly associated information security 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: Section 46 Workbook Q70

[24] The policy must provide for the definition of an access policy with supporting procedures to control the movement of information in and out of the records management systems, allowing the records to be created or viewed by different categories of users: Section 46 Workbook Q69

[25] The policy must require that business continuity plans include provisions for the maintenance of data, information and records and record management processes to ensure a constant service is maintained in spite of any technical or strategic hitches that may occur: Section 46 Workbook Q77 and the policy must define the principle that information held in data, information and records which is considered to be vital to the continuity of the business or urgently required in the event of an emergency should be identified as a matter of priority.: Section 46 Workbook Q82

[26] The policy must make provision for the creation of backups to a corporately agreed standard to include updates for new electronic records and metadata: Section 46 Workbook Q79 and the policy

11. Performance Measurement

The Records Manager will monitor compliance with this policy in liaison with internal audit[27].

12. Review of Policy

This policy will be reviewed on an annual basis.

13. Supporting Documentation

- Information Management Manual[28];
- Information Governance procedures and protocols

14. Related Policies

This policy should be used in conjunction with the following related policies:[29]

- Freedom of Information policy
- Data Protection policy
- Environmental Information Regulations Policy
- Open Data Policy
- Digital Continuity Policy
- Kent and Medway Information Sharing Agreement
- Information Security Policy
- ICT Security Standard
- Electronic Communications Policy
- ICT Security Policy
- Malicious Software Protection Policy

must require the establishment of an effective back-up restoration regime to ensure that when back-ups need to be restored they remain fit for purpose: Section 46 Workbook Q80

[27] Section 46 Workbook Q67

[28] The policy must provide for the development of a framework of appropriate standards, procedures and guidelines to support its implementation Section 46 Workbook Q52

[29] The policy must identify and make appropriate connections to related policies, such as those dealing with email, information security and data protection: Section 46 Workbook Q45

Version Control – Changes made to version 1.1

1. Phone numbers updated to Unified Communications telephone numbers.

2. Section 1: Text removed “underpins the three aims outlined in Bold Steps for Kent and ensures that KCC creates data, information and records which are accurate, reliable and accessible.” and replaced with “supports the implementation of the strategies outlined in Increasing Opportunities, Improving Outcomes: Kent County Council’s Strategic Statement 2015 – 2020 and ensures that KCC creates data, information and records which are accurate, reliable and accessible”

3. Section 3: Footnotes 4 and 5 combined

4. Section 4:

   Following text added: “The SIRO is responsible for ensuring that the appropriate resources are available to implement and monitor the Records Management Policy.”

   Following text removed “The Records Manager is responsible for maintaining the information asset register, the information risk register, the retention schedule and the publication scheme” and replaced with “The Records Manager is responsible for maintaining the information asset register, the information risk register and the retention schedule.”

   Following text removed “The Records Manager is responsible for ensuring that the Records Management Service remains compliant with current record keeping practices. The Head of Libraries and Archives is responsible for managing the day to day running of the Records Management Service” and replaced with “The Head of Libraries Registration and Archives is responsible for managing the day to day running of the Records Management Service. However, the Records Manager is responsible for ensuring that the Records Management Service remains compliant with current record keeping practices”.

5. Section 5: Footnotes 11 and 12 combined. Footnotes 14, 15 and 16 combined.

6. Section 9: Footnotes 26 and 27 combined

7. Section 10: Footnotes 30 and 31 combined. Footnotes 32 and 33 combined.

8. Section 11: Following text removed “All systems and processes dealing with data, information and records should incorporate appropriate performance measures to ensure the quality and reliability of the records to provide a valuable information and knowledge resource for the whole organisation. Audits will be undertaken, where appropriate, of the registration and classification references used by Kent County Council so that the system makes sense and relevant records can be found in appropriate search sequences.” and replaced with “The Records Manager will monitor compliance with this policy in liaison with internal audit.”

Changes made to Version 2

1. Section 5: Text “sections 7-10” replaced with “sections 7-8)

2. Section 7: Text “section 13 of” replaced with “Specialist Guidance 5 in”

3. Section 8: Text “section 12” replaced with “section 9”

4. Section 8: Text “sections 12.2-12.5” replaced with “section 9.4”

Changes made to Version 3

1. All references to the Data Protection Act 1998 replaced with General Data Protection Regulations 2016
2. Version 3.2 Change to the post holder for SIRO and addition of Data Protection Officer

Changes made to Version 3.2

1. “Head of Governance and Law” replaced with Head of Governance, Law and Democracy.

2. “the Information Security Incident Policy & Protocol” replaced with “Data Breach Policy”

3. “General Data Protection Regulation 2016” replaced with “United Kingdom General Data Protection Regulation”