

Records Management, Retention and Disposal Policy and Procedure

<i>Policy Number:</i>	8.1	<i>Version number:</i>	01
<i>Date of issue:</i>	07/11/2017	<i>Date Archived:</i>	
<i>Reason for policy: (Redraft/new)</i>	<i>New policy to ensure compliance with current legislation</i>		
<i>Authorised by:</i> <u>Caroline Allen</u> <i>On Behalf of Management</i>	<i>(Signature)</i>		
<i>Agreed by:</i> <u>Pam Sian</u> <i>On Behalf of UNISON</i>	<i>(Signature)</i>		
<i>Agreed by:</i> _____ <i>On Behalf of Unite</i>	<i>(Signature)</i>		

N.B. The original copy of this policy containing signatures is held in the Human Resources office.

CONTENTS

1.	Introduction.....	3
2.	Policy Purpose.....	3
3.	Related Policies & Employment Legislation	4
4.	General Principles	4
4.1.	Scope.....	4
4.5.	Management of Records	5
4.6.	Retention of Records.....	5
4.7.	Disposal of records.....	7
4.8.	Review of records.....	7
4.9.	Duplicate Records.....	7
4.10.	Transfer of records	8
5.	Procedure.....	8
5.6.	Training and Awareness.....	8
5.10.	Policy Compliance and Audit.....	9
6.	Equality Impact Assessment.....	9
7.	Changes to Policy.....	9

1. Introduction

- 1.1. This policy is a part of a set of Information Governance policies and procedures that support the delivery of the CA's functions and it should be read in conjunction with these associated policies.
- 1.2. A list of related policies, procedures, and strategies and details of how to access them can be found under the 'Policies' section of our Intranet site.
- 1.3. All the CA's records require proper management throughout their lifecycle; from creation to ultimate disposal.
- 1.4. Physical or electronic documents and records may need to be retained in order to fulfil statutory or regulatory requirements, for example the Limitation Act (1980), to evidence events/agreements in the case of dispute(s), to meet operational needs, or to ensure the preservation of documents which have historic or cultural value.
- 1.5. However, keeping records that are not required wastes space, time and energy. Expensive physical and electronic storage space is used, time is wasted in managing these records, and accessibility is slowed, as those records that are not needed get in the way of those that are, i.e. those containing important information.
- 1.6. The untimely destruction of documents to which one or more of the criteria in paragraph 1.3 is applicable, could cause the CA difficulty in defending a claim or prosecution brought against it or could cause operational problems or embarrassment to the organisation. Conversely, retaining records for too long could result in a breach of the Data Protection Act (1998). The permanent retention of all documents and records is undesirable, uneconomical and unsustainable.
- 1.7. This policy outlines the requirements that must be met in order for the CA to ensure that its records are created, captured and managed appropriately to recognised standards.
- 1.8. This policy outlines the need for the CA records to be retained for agreed periods of time, reviewed if necessary, and disposed of according to rules which will be clearly stated on retention schedule documents.

2. Policy Purpose

- 2.1. To outline the standard to which the CA's records must be managed in order to ensure they support the operations of the CA, support accountability processes and provide evidence of business activity;
- 2.2. To enable all staff to recognise the importance of good records management, and to understand their roles and responsibilities with respect to compliance with this policy;
- 2.3. To ensure relevant officers understand their responsibilities with regard to the provision of records management training for staff;
- 2.4. To promote the development and approval of an information asset register which will enable improved and consistent record retention and disposal practices across the CA;
- 2.5. To ensure that the CA only retains records that are required by law or to support the business activity or transactions of the organisation;

- 2.6. To outline the standards that must be met to ensure appropriate retention and disposal of CA records;
- 2.7. To ensure that the CA complies with relevant regulations and legislation, for example the Data Protection Act (1998);
- 2.8. To protect the CA against the business and compliance risks associated with retaining records for too long, or disposing of them too soon;
- 2.9. To promote the identification of records which require permanent preservation to ensure protection of the CA's corporate memory;
- 2.10. To ease pressures on physical and electronic storage space, facilitate fast retrieval of records, and improve staff confidence in records, by reducing the volume of records that are kept unnecessarily;
- 2.11. To ensure that when additional information governance rules (for example security classifications) are applied to records, this is carried out in the most efficient way possible, as these rules will only be applied to records that actually need to be retained.

3. Related Policies & Employment Legislation

- 3.1 Data Protection Policy
Freedom of Information and Environmental Information Regulations Policy
Information Governance Policy
Information Sharing Policy
Subject Access Request Policy
Information Asset Register
- 3.2 We remain up to date and compliant with all current employment legislation.

4. General Principles

4.1. Scope

- 4.2. This policy applies to everyone who has access to the CA's information, information assets or IT equipment. These people are referred to 'users' in this policy. This may include, but is not limited to employees of the CA, temporary workers, partners and contractual third parties. The CA is the accountable body for the Leeds City Region Enterprise Partnership (LEP) which is also covered by this policy.
- 4.3. This policy is relevant to records of the CA. A 'record' is defined as follows:

Information that is **created or received, captured, and maintained as evidence** of the business of the CA, due to its operational, legal, financial, or historical value to the organisation.
- 4.4. This policy covers records in all physical and electronic formats; including, but not restricted to:
 - Paper;
 - Electronic documents;
 - E-mails;

- Voicemail;
- Web records such as blogs, wikis and discussion threads;
- Other records created in social media used for business purposes, such as Twitter;
- Visual images such as photographs
- Scanned images;
- Microform, including microfiches & microfilm;
- Records stored on removable media, such as audio and video tapes, memory sticks, CDs, DVDs and cassettes;
- Published web content (Intranet/Internet); and
- Databases and spread sheets.

This policy will also cover formats that are developed and used in the future.

This policy does not cover documents that are not CA records, for example, non-work related emails, stationery or reference material.

4.5. Management of Records

- 4.4 To help ensure the quality and reliability of records, record creation and content will be standardised where possible and relevant, by the use of templates, version control and naming convention guidelines, and email protocols.
- 4.5 The information contained within records will be accurate and of a high quality, in order for staff to be able to trust the records they use. The CA must be able to prove the authenticity of its records.
- 4.6 Data must be complete, valid, accurate, and consistent across databases. This is to ensure that such data is fit for purpose, and to help ensure the quality of records produced from those databases.
- 4.7 Records should be classified and indexed to ensure that they are available for staff to be able to access them easily and quickly. The way that records are classified will support the interpretation of those records within the relevant context.
- 4.8 Records will be retained for as long as they are required for legislative, business, accountability, or cultural purposes.
- 4.9 Records will be stored in a manner and location that enables the CA to have an appropriate level of control over their management. This level of control must be sufficient to enable the CA to ensure usability, provide evidence of integrity, and ensure records are protected against unauthorised access, loss, or damage.

4.6. Retention of Records

- 4.10 It is a requirement of this policy that all CA records are retained and disposed of in accordance with clear rules agreed between relevant service areas and Legal Services. Rules stating how long records will be kept for (retention periods) will be outlined in the information asset register which will be subject to an annual review. Retention periods should be assigned to existing records retrospectively (as far as possible) and to all newly created records. The information asset register is a working document and is published separately on the CA's internal Intranet site for all users to view and for Information Asset Owners to update as necessary.

- 4.11 The length of the retention period will depend on the type of record and its value to the CA, and any legislation or standards that might apply. Where possible, disposal, review or transfer dates will be recorded on, or within the record or collection of records.
- 4.12 Most records will need to be kept for defined periods of time as per the associate Information Asset Register, however they may be retained for longer periods when:
- The information contained in them is relevant to a legal action which has been started or is pending. It is the responsibility of the service area to provide information about pending legal action, which should be brought to the attention of Legal Services. If such action is pending, a note should be appended to any physical file stating that the records should not be destroyed. Electronic records should be flagged to prevent erasure;
 - They hold business value to the organisation for longer than their normal retention period;
 - They are required to be kept longer by statute. A number of Acts, for example the Latent Damage Act (1986), and regulations govern the retention of certain types of records;
 - They hold historical, cultural, or educational value, and need to be transferred to the West Yorkshire Archive Service for permanent preservation;
 - They consist of information maintained for the purpose of retrospective comparison. For example tracking service improvement or service profiling data;
 - They are required for the purpose of staff disciplinary proceedings; or
 - They relate to contracts 'under seal' between the CA and a third party.
- 4.13 As outlined above, some CA records may have historical, cultural or educational value, to the extent that they must be retained permanently. Records that do not hold such value will not be retained for an indefinite period of time.
- 4.14 Services will follow the CA's guidance for setting retention periods, to ensure that records are kept for long enough to provide a reasonable level of historical information, which may be required for future reference purposes.
- 4.15 The information asset register will be reviewed annually and updated by Information Asset Owners as necessary.
- 4.16 Where records contain personal information, the fifth principle of the Data Protection Act (1998) must be satisfied – 'personal data should not be kept for longer than necessary'.
- 4.17 As far as possible, similar records across the organisation will be held for the same length of time. The Legal and Governance Services team will have an over-arching role in the development of the information asset register, to ensure this consistency is achieved.
- 4.18 The information asset register will take account of any existing schedules during development, and will supersede these once it has been approved, in order to achieve consistency.
- 4.19 Documents that are not CA records should be disposed of once their usefulness has passed.

4.7. Disposal of records

- 4.20 Records must be disposed of appropriately once their retention period has expired. Records should not be retained beyond disposal dates, and therefore services must consider the practicality of disposing of records in accordance with the relevant date.
- 4.21 Retention rules must cover 'archived' data and data held on back up tapes, to ensure clarity over when a record has actually been deleted. The CA's Corporate ICT service are responsible for the destruction of data held on back-up tapes in line with the retention schedule.
- 4.22 Where records are destroyed a record must be kept, containing all the information outlined in the template at [Appendix A](#). Disposal records should demonstrate that the disposal was in accordance with this policy or a written record should be made justifying the reasons for departure from this policy. If records are destroyed by external organisations on behalf of the CA, a certificate of destruction should be provided to, and held by, the relevant Records Manager.
- 4.23 If a record due for destruction is known to be the subject of a request for information under the Data Protection Act (1998), Freedom of Information Act (2000) or Environmental Information Regulations (2004), destruction should be delayed until disclosure has taken place or, if the CA has decided not to disclose the information, until the complaint or appeal provisions of the relevant legislation have been exhausted.

4.8. Review of Records

- 4.24 When a review date is reached, a review should be undertaken to determine if the record can be disposed of, or if a further review or disposal date needs to be assigned. Where records are not destroyed as a result of review, this action, and the reasons for it, must be clearly justified, and documented within the disposal record as outlined in 4.14.
- 4.25 The frequency of review depends upon the retention period as specified in the Retention Schedule.

4.9. Duplicate Records

- 4.26 Many CA records will exist in both electronic and physical formats, and multiple copies may exist. The creation of duplicate records should be kept to a minimum, for example when copies of meeting papers are printed, these copies should be disposed of as soon as they are no longer needed for reference. If duplication is necessary, then a decision must be taken as to which copy is the 'master' copy record, and retention rules should reflect this decision. If one copy is destroyed but others still exist, then the CA still holds the information, and this could increase the risk of a breach of the Data Protection Act (1998), or lead to a failure to comply with a request under the Freedom of Information Act (2000)/Environmental Information Regulations 2004.
- 4.27 Where the decision is taken that an electronic copy is the 'master' copy of a record, then consideration must be given to any potential legal admissibility issues that may arise. For further information please contact the Legal and Governance Services Team.

4.10. Transfer of records

- 4.28 Records that require permanent preservation (refer to 4.12), should be retained by the CA for as long as required to support business processes, and should have an agreed transfer date.
- 4.29 Information Asset Owners should contact the West Yorkshire Archive Service to arrange the secure transfer of such information once this is no longer required to support business processes.

5. Procedure

- 5.1. Any records created by employees of the CA or transferred to the CA by an external organisation, are part of a corporate asset, and are the property of the CA. Individual employees are responsible for ensuring that:
- The policy and any related procedures are adhered to;
 - All records, regardless of format, are managed in line with corporate policy;
 - The information asset register, once approved, is adhered to, and consequently records are disposed of, reviewed, or transferred to the West Yorkshire Archive Service
- 5.2. It is important that all users (as defined in 4.1) understand what is required of them and comply with this policy.
- 5.3. Information Asset Owners will be responsible for:
- ensuring that users are fully informed of their obligations and responsibilities with respect to information governance policies, standards, guidelines and procedures;
 - ensuring that breaches of information governance policies are brought to the attention of the appropriate employee assigned responsibility for information governance, at the earliest opportunity; and
 - ensuring that temporary staff or external contractors only access information required to perform their duties with the CA and are provided information security training before handling any CA information.
 - Ensuring that the correct use of data regardless of whether data is maintained within a software application, SharePoint site or as office documents in a network folder. ICT Services are required to obtain written permission from Information Asset Owners when amending access rights to data (for example, before changes are made to those who can view or amend documents in the Leadership Team folder, written permission must be sought from the Director of Resources).
- 5.4. Information Asset Owners will be responsible for developing, advising and monitoring compliance with record retention and disposal schedules and supervising records access and permission controls, as well as keeping the Information Asset Register accurate and up to date.
- 5.5. The CA's ICT services will be responsible for ensuring that future technologies procured by the CA allow access to electronic records for the duration of relevant retention periods.

5.6. Training and Awareness

- 5.7. Appropriate training will be made available for existing staff that have responsibility for information governance duties.

- 5.8. All staff will be made aware of their obligations for information governance through effective communication programmes.
- 5.9. Each new employee will be made aware of their obligations for information governance during an induction programme.

5.10. Policy Compliance and Audit

- 5.11. Failure to observe the standards set out in this policy may be regarded as serious and any breach may render an employee liable to disciplinary action, which may include dismissal.
- 5.12. Non-compliance with this policy could have a significant effect on the efficient operation of the CA and may result in financial loss and an inability to provide necessary services to our customers. The CA will undertake audits as required to monitor compliance with its information governance policies.
- 5.13. The CA's Information Sharing Policy outlines the circumstances under which external organisations will be expected to comply with this policy. Under these circumstances, the CA may take action against external organisations where a breach of policy has occurred.
- 5.14. Any user who does not understand the implications of this policy or how it may apply to them, should seek advice from their immediate line manager and/or the Legal and Governance Services Team.

6. Equality Impact Assessment

- 6.0 In the creation of this policy, consideration has been given to any possible adverse equality impact for the following groups: disability; gender; gender reassignment; marital status (including civil partnerships); sexual orientation; race; religion or beliefs; age; pregnancy and maternity. The policy is considered to have little or no adverse equality impact.

7. Changes to Policy

- 7.0 The CA reserves the right to amend the details of this policy as required following consultation with recognised trade unions and other relevant parties.

This policy will be monitored and reviewed on an annual basis, to ensure that it meets the needs of the CA and ensure compliance with relevant legislation.

A written request can be made to review this policy at any time, by any of the signatories, giving appropriate reasons for requesting the review.

