

	Record Management Policy			
	Document ID		Status	Approved
	Owner	Quality Manager	Version	1.1
	Author	M Horswell	Version Date	19 Mar 2009

Record Management Policy

Record Management Policy

<insert doc id>

19 Mar 2009 / Approved / 1.1

Amendment History:

Version	Date	Amendment History
1.0	Dec 2008	
1.1	19 Mar 2009	Page 1, Section 1; Reference to UKCHIP <i>Control of Records</i> procedure added

Forecast Changes:

Anticipated Change	When

Reviewers:

This document must be reviewed by the following:

Name	Title / Responsibility	Version	Date Issued	Date Reviewed

Approvals:

This document must be approved by the following:

Name	Title / Responsibility	Version	Date Issued	Date Approved

Distribution List:

Document Status:

This is a controlled document.

Whilst this document may be printed, the electronic version maintained in the central Configuration Management File is the controlled copy. Any printed copies of the document are not controlled.

Related Documents:

These documents will provide additional information.

Ref no	Doc Reference Number	Title	Version
		UKCHIP Procedures Manual	

Glossary of Terms:

List any new terms created in this document.

Term	Acronym	Definition

Contents

1 Introduction.....4

2 Types of Record Covered.....5

3 Record Creation5

4 Record Maintenance5

5 Record Closure6

6 Record Retention and Disposal Arrangements6

1 Introduction

This Policy provides a key component of information governance arrangements for UKCHIP and must be an evolving document because standards and practice will change over time. It will therefore be subject to regular review and updated as necessary.

This Policy must be read in conjunction with the UKCHIP Control of Records Procedures document.

The Introduction to The National Archives' Records Management: Standards and Guidance document states:

'A systematic and planned approach to the management of records within an organisation, from the moment the need for a record to be created is identified, through its creation and maintenance to its ultimate disposal ensures that the organisation has ready access to reliable information. An organisation needs to maintain that information in a manner that effectively serves its own business needs, those of Government and of the citizen, and to dispose of the information efficiently when it is no longer required.'

<http://www.nationalarchives.gov.uk/recordsmanagement/advice/standards.htm>

The Directors are personally accountable for records management within the organisation and in addition UKCHIP needs robust records management procedures to meet the requirements set out under the Data Protection Act 1998. Operational control of the Company's records management will be the responsibility of the Company Secretary.

Records are a valuable resource because of the information they contain. High-quality information underpins the delivery of high-quality services. Information has most value when it is accurate, comprehensive, fit for purpose, up to date and accessible when it is needed. An effective records management service ensures that information is properly managed and is available whenever and wherever there is a justified need for that information, to whoever has an authorised right to access it for a legitimate purpose and in whatever media it is required. Information may be needed:

- to support day-to-day business;
- to support sound administrative and managerial decision making;
- to meet legal requirements, including requests from registrants under subject access provisions of the Data Protection Act;
- to assist all types of audits;

The aims of this Policy are:

- to establish an information governance framework for records management in relation to the creation, use, storage, management and disposal of all types of records;
- to clarify the legal obligations that apply to records held by UKCHIP;
- to explain the actions required by the UKCHIP Board to fulfill these obligations;
- to set out recommended minimum periods for retention of all types of records, regardless of the media on which they are held;
- to meet the records control procedure requirements of ISO 9001;

2 Types of Record Covered

The guidelines contained in this Policy apply to records of all types regardless of the media on which they are held. These may consist of:

- registrant records (electronic or paper based)
- administrative records (including, for example, personnel, financial and accounting records);
- e-mails pertinent to both business functions and registrant processes;
- computerised records;
- scanned records;

3 Record Creation

Records of operational activities should be complete and accurate in order to allow directors, employees and their successors to undertake appropriate actions in the context of their responsibilities, to facilitate an audit or examination of the organisation by anyone so authorised, to protect the legal and other rights of the organisation, its registrants, staff and any other people affected by its actions, and provide authentication of the records so that the evidence derived from them is shown to be credible and authoritative.

Records created by UKCHIP should be arranged in a record-keeping system that will enable the organisation to obtain the maximum benefit from the quick and easy retrieval of information.

Paper and electronic record keeping systems should contain descriptive and technical documentation to enable the system to be operated efficiently and the records held in the system to be understood. The documentation should provide an administrative context for effective management of the records.

The record keeping system, whether paper or electronic, should include a documented set of rules for referencing, titling, indexing and, if appropriate, the protective marking of records. These should be easily understood to enable the efficient retrieval of information when it is needed and to maintain security and confidentiality.

4 Record Maintenance

The movement and location of records should be controlled to ensure that a record can be easily retrieved at any time, that any outstanding issues can be dealt with, and that there is an auditable trail of record transactions.

For records in digital format, maintenance in terms of back-up and planned migration to new platforms should be designed and scheduled to ensure continuing access to readable information.

Equipment used to store current records on all types of media should provide storage that is safe and secure from unauthorised access and which meets health and safety and fire regulations, but which also allow maximum accessibility of the information commensurate with its frequency of use.

A contingency or business continuity plan should be in place to provide protection for all types of records that are vital to the continued functioning of the organisation. Key expertise in relation to environmental hazards, assessment of risk, business continuity and other considerations is likely to rest with information security staff and their advice should be sought on these matters.

5 Record Closure

Records should be closed (i.e. made inactive and transferred to secondary storage) as soon as they have ceased to be in active use other than for reference purposes. An indication that a file of paper records or folder of electronic records has been closed, together with the date of closure, should be shown on the record itself as well as noted in the index or database of the files/folders. Where possible, information on the intended disposal of electronic records should be included in the metadata when the record is created. The storage of closed records should follow accepted standards relating to environment, security and physical organisation of the files.

A record of the destruction of records, showing their reference, description and date of destruction should be maintained and preserved so that the organisation is aware of those records that have been destroyed and are therefore no longer available. Disposal schedules would constitute the basis of such a record.

6 Record Retention and Disposal Arrangements

Many records, even administrative ones, contain sensitive or confidential information. It is therefore vital that confidentiality is safeguarded at every stage of the lifecycle of the record, including destruction, and that the method used to destroy such records is fully effective and ensures their complete illegibility and non-recovery.

This retention schedule details a **Minimum Retention Period** for each type of record. Records (whatever the media) may be retained for longer than the minimum period. However, records should not ordinarily be retained for more than 30 years. Records containing personal information are subject to the Data Protection Act 1998 and especially to the fifth principle which states that "personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes".

The following types of record are covered by this retention schedule (regardless of the media on which they are held, including paper, electronic, images and sound):

- administrative records (including personal, financial and accounting records);
- photographs, slides and other images;
- audio and video tapes, cassettes, CD-ROMs, etc;
- e-mails;
- computerised records; and
- scanned documents

Record Management Policy

<insert doc id>

19 Mar 2009 / Approved / 1.1

Type of record	Minimum retention period in years
Administrative	
Agendas and associated papers of Board, Council and Committees and minutes of those meetings	30
Memoranda and Articles of Association, constitutional documents	None
Business plans	20
Annual reports	3
Manuals, policies and procedures (including previous versions)	10
Nominal rolls (includes current registers, registers of those who fail to renew or are withdrawn after challenge)	2 (max. 6)
Registration accounts for those that start but never finish an application	1 (max. 2)
Major reports	30
Specifications	6
Statistics	3
Project files	3
Project files if the initial value of the project or the estimated value of the content as at the year of production is above £100k	6
Papers of minor or short lived importance	2
Financial	
Annual accounts (final)	30
Accounts minor records	2
Accounts working papers	3
Audit records and reports and follow-up actions	2
Bank statements	2
BACS records	6
Bills, receipts, cleared cheques	6
Budgets	2
Contracts (financial)	6 (after termination)
Invoices and ledgers	6
Records of sales activities	6
Tax documents	6
Information Technology	
Software licences	Lifetime of software
Personnel	
Director Service Agreements	None
Contracts of Employment	None
Consultants agreements	6
Assessor agreements	6
Records of education, training, skills and experience	6