Worcestershire County Council

Information and Records Management Policy

Version 1.0
27 April 2015

worcestershire county council

Document Control

Organisation	Worcestershire County Council
Title	Information and Records Management Policy
Author	Becki Staite, Corporate Information Manager
Filename	Information and Records Management Policy v1-0.docx
Owner	Becki Staite, Corporate Information Manager
Subject	Records management; information security; information management; information legislation
Classification	NOT PROTECTIVELY MARKED
Review date	Next review April 2017
SID Location	http://sid/cms/acs/culture-and-community/cimu/policies-and-strategies.aspx
Equalities Impact Assessment	Screening conducted 24/02/2015; full EIA not required
Approval (by whom and date):	Corporate Information Governance Board (CIGB) 27/04/2015 v1.0

Version History

Revision Date	Reviser	Version	Description of Revision
24/02/2015	Becki Staite	v0-1	First draft
02/03/2015	Becki Staite	v0-2	Revised in line with CIGG comments
27/04/2015	Becki Staite	v1-0	Approval by CIGB

Document Distribution

This document will be distributed to:

Name	Job Title	Email Address
All Staff		

Contents

1. Introduction 4
2. Scope 4
3. Information Management Principles 4
4. Roles and Responsibilities 5
5. Information Asset Owner Responsibilities 5
6. Data Owner Responsibilities 6
7. Records Management Liaison Officers (RMLOs) 6
8. Records Management Principles 7
9. Creation of records and information 7
10. Maintenance and Storage of records and information 7
11. Disposal 7
12. Access and Security 8
13. Training and Awareness 8
14. Breaches 8
15. Performance Management 9
16. Policy Review and Revision 9
17. Related Legislation, Standards, and Corporate Policies 9
Appendix 1 Glossary 10
Appendix 2 IM Responsibility Structure and Operational Support Arrangements 11

1. Introduction

1.1 Worcestershire County Council [the Council] recognises that its records and information are an important public and corporate asset, and are a key resource required for effective operation and accountability.

1.2 Changes in legislation have heightened the need for careful management of information and this policy sets out the Council's responsibilities and activities to achieve this. This will ensure the Council creates and captures authentic and reliable records to demonstrate evidence, accountability and information about its decisions and activities.

2. Scope

2.1 This policy applies to all employees and workers (both contracted and agency workers), contractual third parties and commissioned providers, volunteers, and councillors (when acting on behalf of the Council).

2.2 This policy applies to all information created or held by, or on behalf of, the Council, in whatever format or however it is stored. A record is any recorded information regardless of medium (including, but not limited to, paper, microform, electronic and audio-visual), which is created, collected, processed, used, stored and / or disposed of in the course of a Council activity, as well as those acting as its agents in the course of a Council activity.

3. Information Management Principles

3.1 The culture of the Council will be one that uses and promotes good information management practices:

- Information will be managed as a corporate resource and structured to facilitate information sharing across the Council and with our partners where appropriate
- Information will be accurate and up to date to support the Council's operations and decision making process and the needs of our partners
- The creation, storage and use of information will conform to legal and regulatory requirements as well as any Council guidelines and policies
- Information will be captured and stored only once and, where possible, reused as many times as is needed. Where the duplication of information is unavoidable then a single authoritative source must be identified and measures put in place to ensure consistency
- Employees, customers, councillors and all other stakeholders will be able to access the information they require, given any security or legal restrictions. Confidentiality will be respected and restricted information suitably protected.
- The electronic storage and transmission of information will be promoted where there is a clear business benefit in doing so to improve efficiency and consistency of information presentation across all stakeholders.
- Information will be managed in a secure fashion, ensuring the continuity of operations and minimising the possibility of damage to service provision by limiting the impact of security threats or incidents, whether internal, external, deliberate or accidental.
- Information will be regularly reviewed and only be retained where there is a requirement or relevance. Information will be disposed of (securely destroyed or archived) in a systematic way and in accordance with the Disposal Schedule
- Knowledge will be captured and re-used as a matter of process and procedure so that what we know what can be shared and when - both across the Council and with others

4. Roles and Responsibilities

4.1 The Council has a corporate responsibility to maintain its records and record-keeping systems in accordance with legislative requirements.

4.2 The Senior Information Risk Owner (SIRO) has responsibility for setting strategic direction and approving a framework for managing and overseeing duties in relation to records management as set out in this policy. The SIRO is supported in this role by the CIGB and CIGG.

4.3 The Corporate Information Governance Board (CIGB), chaired by the SIRO, shall provide overall direction for information and records management and ensure policies and processes are in place for its safe management.

4.4 The Corporate Information Governance Group (CIGG) shall support the work of the SIRO and the CIGB.

4.5 The Corporate Information Manager will co-ordinate the activities of the Corporate Information Management Unit (CIMU), such as maintaining the corporate Disposal Schedule, managing the physical records storage areas and advising best practice for electronic recordkeeping.

4.6 Worcestershire Archives and Archaeology Service, the Place of Deposit for Public Records in Worcestershire, will take custody of those records deemed worthy of permanent preservation.

4.7 Directors are responsible for the management of their Directorate records in accordance with this policy, and ensuring that all staff are aware of their record keeping responsibilities.

4.8 Commissioning Managers and Heads of Service are responsible for considering information management implications when planning to commission services to external providers, work with partners, commission new technologies or major structural changes.

4.9 Information Asset Owners (IAOs) are responsible for ensuring appropriate information management practices are in place for their information assets (electronic and paper). The role is further defined in section 5.

4.10 Data Owners (DOs) are the business managers who support the Information Asset Owners and operationally own the information and records contained in their systems (paper and/or electronic). Their role is to understand what information and records are held, how they are used and transferred, and who has access to them and why, in order for business to be transacted within an acceptable level of risk. The role is further defined in section 6.

4.11 Records Management Liaison Officers (RMLOs) are staff who support the Data Owner in the practical management of their business unit and have specific responsibilities for records management in their business units and this responsibility will be clearly defined in their job descriptions. See also section 7.

4.12 All Council employees, elected members, contractors, consultants and agents are responsible for creating and maintaining records in relation to their work that are authentic, reliable and for documenting their decisions and actions; managing information in accordance with this policy and any related procedures; and ensuring that the key records they are responsible for remain accessible.

5. Information Asset Owner Responsibilities

5.1 The Information Asset Owner role, in order for business to be transacted within an acceptable level of risk, includes, but is not limited, to:

- understanding what information is held and how it is used;
- determining the business requirements for the use of the information and signing them off;
- determining who has access to it and why, and signing off the access privileges;
- ensuring information and systems are prioritised in line with their importance to the organisation;
- defining information sharing agreements and data interchange agreements ensuring adherence to the provisions in appendix 3 of the Information Classification Policy;
- developing service level agreements in relation to the information;
- assigning the information classification to the asset (based on the content and impact of disclosure, see appendix 2 of the Information Classification Policy for criteria);
- authorising disclosure of information from the systems to third parties;
- identifying and authorising amendments to the Disposal Schedule;
- authorising new or significant changes to the system;
- being involved in security audits and reviews;
- ensuring users are aware of their responsibilities and can fulfil them.

5.2 When a nominated Information Asset Owner leaves the council, the role will be transferred to their successor – either the next person appointed to the post, or the person who takes on responsibility for the business processes dependent on the information and systems. In the event of an interim period, the responsibility will lie with the original Information Asset Owner's line manager.

5.3 The Information Asset Register must be updated with any changes, updates or amendments to Information Asset Owners.

6. Data Owner Responsibilities

6.1 Information Asset Owners may delegate day-to-day maintenance of information assets to Data Owners to ensure they are managed appropriately, but they remain accountable for the actions taken.

6.2 When a nominated Data Owner leaves the council, the role will be transferred to their successor – either the next person appointed to the post, or the person who takes on responsibility for the business processes dependent on the information and systems. In the event of an interim period, the responsibility will lie with the original data owner's line manager. CIMU must be notified of any changes, updates or amendments to nominated data owners.

7. Records Management Liaison Officers (RMLOs)

7.1 RMLOs provide a formal link between business units, teams and CIMU through which the implementation of records management best practice and procedures can be disseminated. Areas of responsibility include:

- Monitoring use of the Corporate File Plan
- Receipt and allocation of duplication reports and ensuring follow-up action is taken
- Adherence to the Disposal Schedule
- Induction for new starters into records management principles and procedures
- Housekeeping and maintenance of records management practices
- Liaison with CIMU in regard to local management of records

8. Records Management Principles

8.1 Maintaining appropriate and effective records management practices will help us to deliver our priorities and fulfil our statutory duties. The adoption of this policy will ensure our records, whatever format they are in, are accurate, reliable, ordered, complete, useful, up to date and accessible whenever they are needed.

8.2 The underlying principle of records management is to ensure that a record is managed through its life cycle from creation or receipt, through maintenance and use to disposal.

8.3 Good records management relies on the following:

- the creation of appropriate records
- the capture of records (received or created) in record keeping systems
- the appropriate maintenance and upkeep of these records
- the regular review of information
- controlled retention and disposal of information

8.4 Through adhering to these principles we will benefit from:

- records being easily and efficiently located, accessed and retrieved
- information being better protected and securely stored
- records being disposed of safely and at the right time

9. Creation of records and information

9.1 Records will be created which document the Council's principal activities and which are required to evidence business, regulatory, legal and accountability purposes.

9.2 Records will be created with meaningful titles and indexes/metadata so that they can be retrieved quickly and efficiently.

9.3 All record creators will ensure such records are authentic, reliable, have integrity and remain usable. This includes making appropriate arrangements for ensuring the continuity and availability of information when staff leave, or during major organisational or technological change.

10. Maintenance and Storage of records and information

10.1 Electronic and paper systems containing records must be maintained so that the records are properly stored and protected, and can easily be located and retrieved. There must be procedures to ensure the systems contain accurate information. The systems must also take into account the legal and regulatory environment specific to their area of work.

10.2 The Corporate Information Management Unit (CIMU) provide a secure storage facility that must be used to store physical records which are not being actively worked on, but do need to be retained for business, regulatory, legal and accountability purposes (semi-current physical records).

10.3 The Corporate File Plan must be used to store electronic records that are not held in corporate databases or systems (examples of such systems include Frameworki and SAP).

11. Disposal

11.1 With increasing public access to our records, it is important that disposal of records happens as part of a managed process and is adequately documented. Information Asset Owners must have in place clearly defined arrangements for the identification and selection of records for disposal, and for documenting this work.

11.2 The Disposal Schedule is the principal authority on the retention of records in all formats in Worcestershire County Council and was ratified as such by the Chief Officers' Management Board (COMB) in June 2001. Amendments to the Disposal Schedule are coordinated by CIMU following advice from the relevant service areas.

11.3 Electronic records must be managed in accordance with the Disposal Schedule. All new computer systems must include the functionality to delete single records or groups of records at the end their retention period. It is recommended that an intended disposal or review date is captured when creating electronic records.

11.4 Any records or information subject to a current Data Protection, Freedom of Information, or Environmental Information Regulations request should not be destroyed and the disposal process should be put on hold until the completion of the request(s).

12. Access and Security

12.1 All Council records will be subject to appropriate security measures as set out in the Council's Information Security Policy. The Council needs to ensure that decisions regarding access to the records are documented so that they are consistent, and can be explained and referred to.

12.2 Data Owners must ensure that:

- All staff are aware of the arrangements for allowing access to certain types of information.
- Procedures are in place to document decisions concerning access.

12.3 By default, no user should have access to systems containing personal information. Users should only access systems and records containing personal information that are relevant to their work/duties. Where access is deemed necessary, the level of access should be determined using the 'need to know' principle ie. to the smallest possible sub-set of records.

13. Training and Awareness

13.1 All Council employees are involved in creating, maintaining and using records and it is important that everyone understands their information management responsibilities. Managers will ensure that staff responsible for managing records are appropriately trained or experienced and that all staff understand the need for records management.

13.2 Training and guidance is available for staff to provide them with the knowledge and tools to effectively and appropriately manage their records.

- Information Governance Training
- Guidance - Managing Your Records

13.3 A mandatory training programme is in place for all staff to ensure they are aware of their obligations under information legislation (Data Protection, Freedom of Information and so on).

14. Breaches

14.1 Non-compliance with this policy may leave the Council vulnerable to legal action and / or reputational damage.

14.2 Any breaches of this policy will be dealt with in accordance with the County Council's procedure for dealing with poor performance and misconduct. Managers will need to decide what action is appropriate based on the circumstances and may wish to seek advice from their HR Manager, and the Corporate Information Management Unit.

15. Performance Management

15.1 The Corporate Information Management Unit will monitor performance with regard to the storage, retention and retrieval of physical records held in its custody.

15.2 Internal Audit will monitor compliance with this policy across the Council.

16. Policy Review and Revision

16.1 This policy will be reviewed as it is deemed appropriate, but no less frequently than every 2 years.

16.2 Policy review will be undertaken by the Corporate Information Manager in consultation with the Corporate Information Governance Group, and relevant directorate representatives.

17. Related Legislation, Standards, and Corporate Policies

17.1 The Council have a legal obligation to comply with the following relevant legislation:

- Public Records Act 1958
- Public Records Act 1967
- Local Government Act 1972 s.224
- Local Government (Access to Information) Act 1985
- Local Government (Inspection of Documents) Order 1986
- Freedom of Information Act 2000
- Data Protection Act 1998
- Environmental Information Regulations 2004
- Computer Misuse Act 1990
- Freedom of Information Act 2000
  (This list is not exhaustive.)

17.2 Relevant Standards

- Lord Chancellor's Code of Practice on the Management of Records under Section 46 FoIA
- ISO 15489 Information and Documentation - Records Management
- BS 10008:2008 Evidential weight and legal admissibility of electronic information
- BIP 0008 Code of practice for legal admissibility and evidential weight of information stored on electronic document management systems
- Data Handling Guidelines for Local Government

17.3 The following Council policy and strategy documents are directly relevant to this policy:

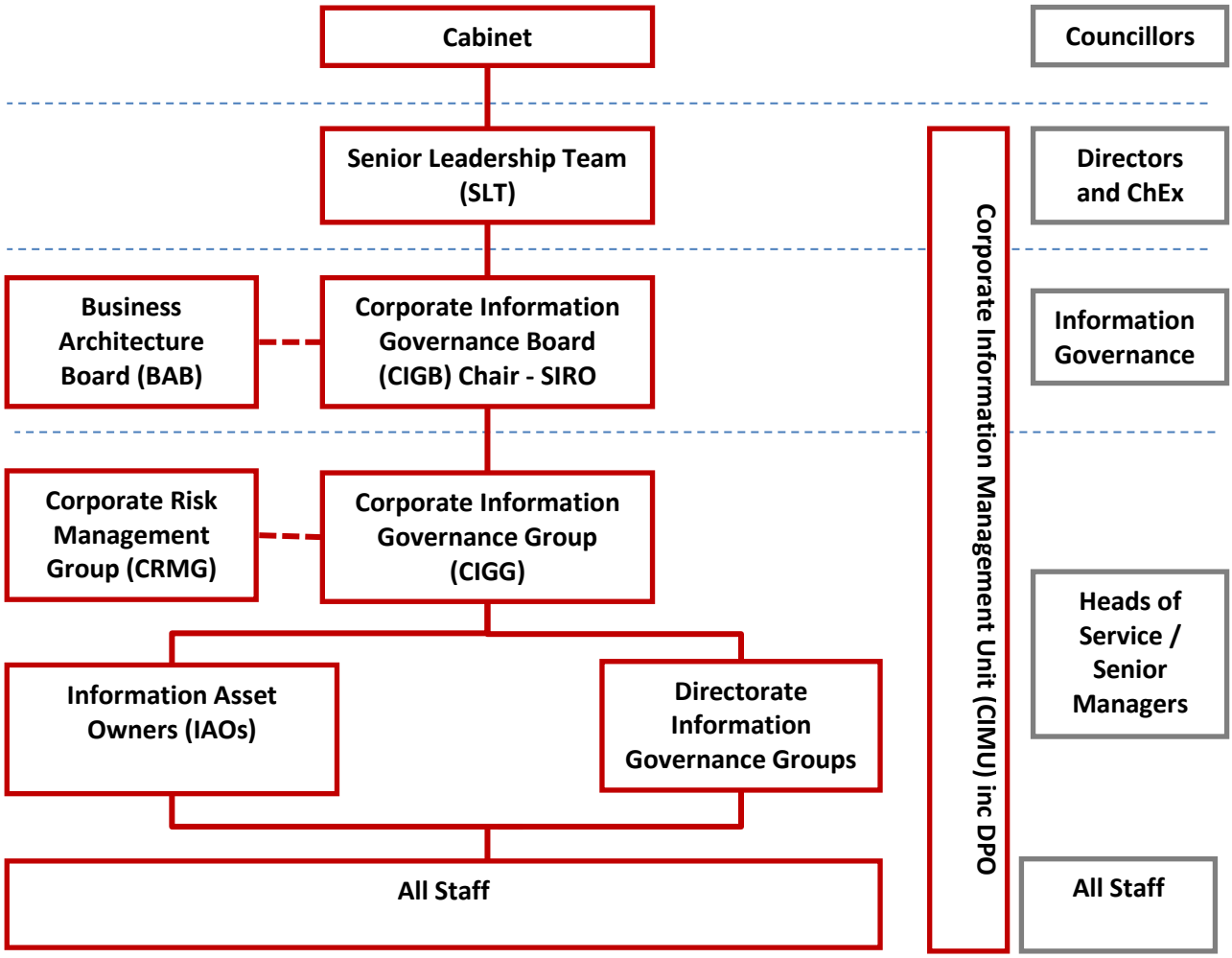
- Information Governance Strategy 2014-2017
- Digital Strategy 2013-2017
- Information Security Policy
- Information Classification Policy
- Freedom of Information and Environmental Information Policy
- Data Protection Policy
- WAAS Acquisition and Collection Policy

Appendix 1 Glossary

Corporate File Plan	The logical arrangement of documents or files that has been adopted by the Council to manage our records, allowing easier identification, storage and retrieval of information. Essentially it is a direction or set of pointers to help you find information/what you want
Disposal	Either secure destruction or permanent preservation of records at the end of their business use
Record	Any recorded information regardless of medium (including, but not limited to, paper, microform, electronic and audio-visual), which is created, collected, processed, used, stored and / or disposed of in the course of a Council activity
Semi-current records	Records which are not being actively worked on, but do need to be retained for business, regulatory, legal and accountability purposes

Appendix 2 IM Responsibility Structure and Operational Support Arrangements

Responsibility Structure



Operational and Support Role Arrangements