INFORMATION & KNOWLEDGE MANAGEMENT

APPENDIX 1

Leeds City Council
Information Governance Framework

October 2008

Contents

Introduction

Section 2 – Policy and Compliance Environment

Section 3 – Information Governance Needs

Section 4 – The Information Governance Framework

Section 5 – Support Arrangements

Appendices

INFORMATION & KNOWLEDGE MANAGEMENT

Leeds City Council Information Governance Framework

Introduction

INTRODUCTION

1.1 What is Information Governance?

1.1.1 Information Governance provides a framework for bringing together all of the requirements, standards and best practice that apply to the handling of information.

1.1.2 The scope of Information Governance, taken at its widest, includes the management of information in all locations and all media. It includes structured information in databases and unstructured information in paper and electronic files. It includes emails and transient documents, work in progress and telephone notes. It includes blogs, wikis and discussion threads. It includes vital records essential to the continuation of Council business and long-term records that must be preserved through many generations.

1.1.3 Information Governance is about records management, about compliance and also about efficient ways of handling of information.

1.1.4 The acronym 'HORUS' reminds us of what this means: -

- **H**olding information securely and confidentially
- **O**btaining information fairly and efficiently
- **R**ecording information accurately and reliably
- **U**sing information effectively and ethically
- **S**haring information appropriately and lawfully.

1.2 Purpose

1.2.1 This document forms the core of Leeds City Council's Information Governance Framework.

1.2.2 Information is one of the Council's most important assets, alongside its people, property, capital and technology. In this regard Information Governance is identified both as a core principle within the Council's Corporate Governance Statement and as being fundamental to the delivery of the Council's strategic Information and Knowledge Management agenda.

1.2.3 The purpose of the Framework is to provide the council with a set of objectives to define its approach to Information Governance and set out all the policies, standards and best-practice which apply to the handling of information, and which are needed to deliver the Information Governance objectives.

1.3 Document Structure

1.3.1 The document is structured as follows:

Section 2 – Policy and Compliance Environment

1.3.2 This section defines information Governance and why it is important to the Council. It also outlines the internal and external drivers behind why the council, like most other organisations, is endeavouring to strengthen its Information Governance practices.

Section 3 – Information Governance Needs

1.3.3 This sections outlines what issues need to be addressed when looking at information Governance. It covers those Information Governance 'needs' that are prerequisite issues that must be addressed through the Framework.

Section 4 – The Information Governance Framework

1.3.4 This section outlines in more detail the rationale, objectives and policies and procedures required to help deliver each of the six areas that make up the Information Governance Framework.

Section 5 – Support Arrangements

1.3.5 This section details the arrangements in place to support delivery of the Information Governance Framework. Principally the focus is on ensuring the requisite skills and competencies exists within the Council to manage, use and share information appropriately and that appropriate Stewardship arrangements are in place to maintain adherence to the Information Governance Framework.

Appendices

1.3.6 There are two appendices to support the Framework. The first provides an information Governance Toolkit which enables a baseline assessment to be made across each of the six authorities with tools and techniques (to be developed) to improve from the baseline towards delivery of the objectives. The second is the Information Governance Workbook, a practical and pragmatic tool which enables service areas across the Council to address practical aspects of Information Governance pertaining principally to Document and Records Management.

INFORMATION & KNOWLEDGE MANAGEMENT

Leeds City Council
Information Governance Framework

Section 2

Policy and Compliance Environment

POLICY AND COMPLIANCE ENVIRONMENT

2.1 Legislative and Regulatory Drivers

2.1.1 The requirement for Information Governance in local authorities is laid down principally by two Acts of Parliament: the Freedom of Information Act and the Data Protection Act.

Freedom of Information Act 2000 and Environmental Information Regulations

2.1.2 The Freedom of Information (FOI) Act has 'raised the bar' for Information Governance in the public sector.

2.1.3 FOI makes the presumption of open access to records with the exception of defined exemption categories. The public has the right to see records, either copies or originals, as well as a summary of information if the applicant so requests and must receive a response within 20 working days

2.1.4 FOI also requires public bodies: -

- to follow codes of practice for records management
- to draw up an Information Asset Register
- to provide a publication scheme.

2.1.5 The Environmental Information Regulations (EIR) came into effect the same time as FOI. These differ from FOI in that they apply only to environmental matters, although their scope is wide enough to include buildings and grounds. In addition to written requests EIR requests may be made verbally by telephone or visit. EIR requests must also be answered within 20 working days.

2.1.6 FOI and EIR access requests may require information from any source: data systems or electronic documents or paper files, active or archived, or email folders, PC drives, CD-ROMs, microfiche or shared drives. Requests may be made for current or retrospective information and although there is a limit on the effort expendable (around 2.5 days) the difficulty in assembling information due to a lack of good record keeping is not an acceptable exemption category.

2.1.7 The impact of the Act on Information Governance lies mainly in Section 45, the discharge of functions, and Section 46, the management of records. The then Lord Chancellor issued two Codes of Practice to interpret the law and assist with compliance: one for Section 45[1] and one for Section 46[2].

2.1.8 The Code of Practice under Section 46 requires public sector organisations to have: -

- 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 between systems);
- the application of appropriate disposal procedures, including procedures for archiving;
- the ability to cross reference electronic records to their paper counterparts in a mixed environment;
- a record keeping system.

2.1.9 The Freedom of Information Act and the Data Protection Act (see below) are enforced by the Information Commissioner; however the enforcement of the Section 46 records management

[1] Secretary of State for Constitutional Affairs' Code of Practice on the discharge of public authorities' functions under Part I of the Freedom of Information Act 2000 Issued under section 45 of the Act November 2004 www.dca.gov.uk/foi/reference/imprep/codepafunc.htm

[2] Lord Chancellor's Code of Practice on the Management of Records Issued under section 46 of the Freedom of Information Act 2000 November 2002 www.dca.gov.uk/foi/reference/imprep/codemanrec.htm

requirements and the Lord Chancellor's Code of Practice has been delegated to the National Archives (TNA).

2.1.10 The principal method for monitoring conformance will be self-assessment but the Commissioner may request the TNA to carry out assessments of conformity with the Records Management Code on his behalf. Selected authorities may be actively audited by the TNA, in accordance with guidelines set out by the Commissioner.

2.1.11 The National Archives have produced an Evaluation Workbook to enable local authorities and other public bodies to self-assess their compliance with the Code of Practice[3].

Data Protection Act 1998

2.1.12 The Data Protection Act (DPA)[4] also makes high demands of an authority's Information Governance, both in terms of records management and in terms of the council's duty to respond to subject access requests.

2.1.13 The Act provides for the protection for personal data and subject rights of access. Personal data is defined as information about a living person who can be identified from the data or from the data and other information (e.g. combination of address and electoral roll)

2.1.14 The 8 principles of good practice stipulate that personal data must be: -

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Not kept longer than necessary
- Processed in accordance with the data subject's rights
- Secure
- Not transferred to countries without adequate protection.

2.1.15 The Act increases the necessity for control of content, retention, security and access to subject files. Its powers have been introduced progressively but will apply fully to all personal data in all media by October 2007.

2.1.16 The main impact of the Act on Information Governance is that it limits the retention of personal information. To comply with the Act the Council must have an approved retention schedule for each type of personal information and evidence that it has complied with the schedule. The length of the retention schedule is not prescribed by the Act but the Council must be able to justify it on the grounds of statutory requirements and business need.

2.1.17 The Act requires the Council to have procedures for classifying personal information and disposing of it. This includes paper files, electronic case records and emails that contain personal information. Email archiving systems and backup tapes are not exempt from the Act. They may be in breach of the Act if they keep information too long and they may need to be searched for information in response to a subject access request.

2.1.18 The duty to respond to subject access requests within 40 days is less of a challenge than the 20 working days of the FOI access request. The scope of the search is limited to information in a 'relevant filing system'. A court case in 2004[5] clarified which manual files count as a 'relevant filing system' limiting them to any records structured so that information relating to an individual is readily accessible.

2.1.19 The Data Protection Act is frequently cited as a reason for not sharing information and joining up information between services. In fact there are many good reasons for sharing personal information, not least the convenience of the citizen who only might in future have to provide a piece of information only once to the Council, instead of once to each service. Provided that information is not

[3] Complying with the Records Management Code: Evaluation Workbook and Methodology www.nationalarchives.gov.uk/documents/full_workbook.pdf

[4] Data Protection Act 1998 www.opsi.gov.uk/acts/acts1998/19980029.htm

[5] Durant v Financial Services Authority 2004

sensitive, there are very few barriers to sharing personal information within the Council, and information protocols can be set up for sharing with outside organisations.

Other legislation

2.1.20 The Local Government Act 1972 broadly sets out a local authority's requirement to manage documents properly:

> *'a principal council shall make proper arrangements with respect to any documents that belong to or are in the custody of the council or any of their officers.'*

2.1.21 Most other legislation affects Information Governance by specifying the content and retention of specific types of records.

2.1.22 There is a long list of Acts of Parliament that set periods of legal liability and hence dictate minimum retention requirements for related records, including for example: -

- Occupiers Liability Act 1957
- Employers' Liability (Compulsory Insurance) Act 1969
- Taxes Management Act 1970
- Equal Pay Act 1970
- Health and Safety at Work etc. Act 1974
- Sex Discrimination Act 1975
- Race Relations Act 1976
- Limitation Act 1980
- Social Security Contributions & Benefits Act 1992
- Value Added Tax Act 1994
- Education Act 1994
- Disability Discrimination Act 1995
- Data Protection Act 1998
- Adoption and Children Act 2002
- Children Act 2004

2.1.23 In addition to Acts of Parliament there are at least 20 Statutory Instruments that directly or indirectly set retention requirements for records.

2.1.24 Lastly, where the Council has information that is of interest to the public sector, it must comply with the Re-use of Public Sector Information Regulations 2005[6], which is a set of regulations drawn up to encourage the re-use of public sector information by the private sector and to remove obstacles that stand in the way. The main themes of the regulations are improving transparency, fairness and consistency. A Guide to the Regulations and Best Practice explains the Regulations and provides information about existing best practice and sources of help[7].

2.2 Government Guidance

2.2.1 In addition to the legislation, there is also a body of government guidance in the field of Information Governance, both for corporate information management and for specific local services.

ISO 15489

2.2.2 ISO 15489[8] is the international standard for developing a records management programme.

2.2.3 ISO 15489 was agreed in 2001 as the UK national standard for public sector organisations. It is recommended in the Lord Chancellor's Code of Practice on the Management of Records under Section 46 of the FOI Act (see above).

[6] Re-use of Public Sector Information Regulations 2005 Act www.opsi.gov.uk/si/si2005/20051515.htm

[7] The Re-use of Public Sector Information: A Guide to the Regulations and Best Practice www.opsi.gov.uk/advice/psi-regulations/advice-and-guidance/guide-to-psi-regulations-and-best-practice.doc

[8] BS ISO 15489-1:2001 Information and documentation. Records management General www.bsi-global.com/en/Shop/Publication-Detail/?pid=000000000030055690

2.2.4 The standard covers policies and responsibilities for records management, strategies and designs for a record-keeping system with processes and controls, monitoring, auditing and training. It follows the Australian 'DIRKS' methodology which provides a systematic approach to records management involving an information audit, business classification, assessment of existing systems, development of a records management policy and the design of a new record keeping system.

2.2.5 ISO15489 requires a functional business classification scheme which divides records by the functions, activities and transactions to which they belong. It requires the definition of retention schedules, classification of security levels and rights of access, and vocabulary controls for titles and description fields.

2.2.6 ISO15489 was required of local authorities by one of the then ODPM's e-Government Priority Service Outcomes (G19). G19 made adoption of ISO 15489 mandatory. The Priority Service Outcomes are no longer being measured, but the requirement to meet ISO 15489 has not gone away. The TNA is now tasked with monitoring compliance with Section 46 of the FOI Act and has produced a workbook (see the FOI section above) for self-assessment.

2.2.7 Implementation assistance is available from the British Standards Institution: 'BIP 0025-2:2002 Effective records management Practical implementation of BS ISO 15489-1[9].

ISO 17799 / 27000

2.2.8 ISO 17799[10] is a Code of practice for information security management, now being progressively replaced by the ISO 27000 series, of which the first to be issued was ISO 27001[11], replacing part 2 of ISO 17799.

2.2.9 ISO 17799 was mandated for central government by the Office of the e-Envoy (now disbanded). While its status for local government is less mandatory, the standard is recommended as best practice in several places in government guidance.

2.2.10 ISO 17799 treats security as a number of 'controls' including: -

- intellectual property rights
- safeguarding of organisational records
- data protection and privacy of personal information
- information security policy document
- allocation of information security responsibilities
- information security education and training
- reporting security incidents
- business continuity management

2.2.11 The scope of ISO 17799 is much wider than the security of computer systems. It covers human resources, the physical security of storage locations, disaster recovery measures and intellectual property rights.

2.2.12 ISO 27000 treats security in a more systematic fashion, with the aim of building an 'Information Security Management System' that can be audited.

2.2.13 Both 17799 and 27000 have certification schemes for self-certification or external certification.

Information for Social Care

2.2.14 Social Care has needs for Information Governance beyond those of other services. The Department of Health is running an 'Information for Social Care' project[12] to define and assist with information and information systems in Social Services.

[9]BIP 0025-2:2002 Effective records management Practical implementation of BS ISO 15489-1' http://www.bsi-global.com/en/Shop/Publication-Detail/?pid=000000000030103890

[10] BS ISO/IEC 17799:2005 Information technology. Security techniques. Code of practice for information security management. From www.bsi-global.com

[11] BS ISO/IEC 27001:2005 Information technology. Security techniques. Information security management systems. Requirements. From www.bsi-global.com

[12] Information for Social Care web site www.dh.gov.uk/en/Policyandguidance/Informationpolicy/Informationforsocialcare/index.htm

2.2.15 The main requirements are set by the Electronic Social Care Record (ESCR) and the Caldicott Principles.

2.2.16 The ESCR is a Department of Health initiative driven by the e-Government agenda, plus reports such as that of Lord Laming (Victoria Climbié) inquiry and the subsequent Children Act. The purpose was to create standard formats and standard metadata that will enable documents to be available wherever need and shared between local authorities, hospitals, police, schools and other parties involved in social care.

2.2.17 In 2003 the Department of Health issued local authorities with target dates for the introduction of the Electronic Social Care Record: -

- October 2004 – 20% of authorities to use ESCR for new cases
- October 2005 – remaining authorities to use ESCR for new cases
- April 2006 – all authorities to use ESCR to capture audio and video for new cases
- October 2006 – all authorities to capture back-files of current cases into the ESCR.

2.2.18 The ESCR comprises both structured data in data systems and unstructured data (documents).

2.2.19 The main guidance document on the ESCR is the Department of Health's publication 'Defining the Electronic Social Care Record'[13], December 2003. This creates a document-centric view of the ESCR.

2.2.20 The Caldicott Principles[14] cover the management of patient information in the NHS and service user information in Social Care: -

- Justify the purpose (or purposes)
- Do not use patient information unless it is absolutely necessary
- Use only the minimum necessary patient-identifiable information
- Access to patient-identifiable information should be on a strict need-to-know basis
- Everyone with access to information should be aware of their responsibilities
- Understand and comply with the law.

2.2.21 The Caldicott guidance recommends the use of codes rather than names to minimise the amount of patient-identifiable information.

2.2.22 A Caldicott Guardian must be appointed to ensure compliance with the principles.

2.3 Technical standards

2.3.1 For services implementing technology solutions to support Information Governance (e.g. EDRM systems), there are a number of standards that the implemented systems should comply with.

E-government Interoperability Framework (E-GIF) – v6.1

2.3.2 e-GIF[15] prescribes the policies and technical specifications that act as the foundation of the e-Government strategy. e-GIF architecture is made up of the Framework itself plus the e-GIF registry, which contains the e-Government Metadata Standard (e-GMS), the Government Data Standards Catalogue (GDSC), XML schemas and the Technical Standards Catalogue.

2.3.3 Key requirements of e-GIF are: -

- the adoption of the Internet and World Wide Web for government systems
- the adoption of XML and XSL as core standards for data integration and presentation
- web browser as the key interface for access to information
- e-Government Metadata Standard (see Metadata Standards below)
- Government Data Standards Catalogue (GDSC).

[13] 'Defining the Electronic Social Care Record' 2003 'http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4069421

[14] Caldicott Principles http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_062722

[15] E-Government Interoperability Framework 6.1 www.govtalk.gov.uk/schemasstandards/egif.asp

2.3.4 The e-GIF paper is followed by XML schemas for individual applications. These are published on the www.govtalk.gov.uk site.

2.3.5 e-GIF mandates the use of e-GMS metadata on public sector information resources such as EDRM systems and web sites. The Government Data Standards Catalogue GDSC[16] mandates the content of some of that metadata, standardising references used for people, places, property and other identifiers.

E-GMS Metadata Standards

2.3.6 The E-Government Metadata Standard (currently e-GMS v3.1[17]) prescribes standard fields for content management systems. The use of standard fields is mandatory for all EDM and EDRM systems currently being specified in the UK public sector and applies to all interoperation between UK government and public sector, businesses and citizens. It makes document searches more effective on the Internet and in internal content management systems and will apply common standards for metadata as well as standards formats for the document itself.

2.3.7 There are now 25 fields in the e-GMS, based on the metadata elements known as the Dublin Core. The core elements are mandatory, in as much as they must always be completed. Other elements must be configured into the solution, but their completion is optional. Individual implementations may add their own fields to those core elements.

2.3.8 The 25 fields are: -

Accessibility	Digital Signature	Publisher
Addressee	Format	Relation
Aggregation	Identifier	Rights
Audience	Language	Source
Contributor	Location	Status
Coverage	Mandate	Subject*
Creator*	Preservation	Title*
Date*	Publisher	Type
Description		

2.3.9 The elements marked with an asterisk require mandatory completion. Although the mandatory elements are few in number each one may have a number of mandatory refinements such as Date.Created, Date.Acquired and Date.Declared for records and Date.Opened and Date.Closed for folders.

2.3.10 The e-GMS 3.1 fields are included in the 2004[18] update of the National Archives metadata standards for Electronic Records Management Systems.

2.3.11 The 3.1 version of e-GMS has replaced previous options for completion of the Subject field to enforce the use of at least one term from the Integrated Public Sector Vocabulary (IPSV)[19], which is a merger of the GCL (Government Category List), LGCL (Local Government Category List) and seamlessUK taxonomy for web sites. IPSV must be used to populate the e-GMS Subject fields in website metadata, electronic document and record management systems, content management systems, and all situations which manage electronic information and services.

[16] Government Data Standards Catalogue www.govtalk.gov.uk/gdsc/html/frames

[17] E-Government Metadata Standard 3.1 www.govtalk.gov.uk/schemasstandards/metadata.asp

[18] 'National Archives' Requirements for Electronic Records Management Systems: 2: Metadata Standard 2004'

www.govtalk.gov.uk/documents/Records_management_metadata_standard_2002.pdf

[19] IPSV www.esd.org.uk/standards/ipsv/

2.3.12 Any document management system implemented in the Council must include the 25 e-GMS elements and ensure that the mandatory elements are completed as appropriate whether at folder or document level. The system should be able to pass the e-GMS data through to the intranet or internet or export it with the document for information sharing. The system must enforce the use of the IPSV in the Subject field by offering the list as a thesaurus of options during the creation of new folders. There is an ISO standard (ISO 2788, see below) governing the use of a monolingual thesaurus.

2.3.13 Most of the document-level metadata fields can be automatically supplied from Windows system data and Office document properties, and the system implementation should ensure that field completion is automated as much as possible. The folder structure of an EDRM system assists by enabling documents to inherit metadata from their parent folder and class.

National Archives 'Requirements for Electronic Records Management Systems'

2.3.14 The National Archives (TNA) has in the past specified the requirements for Electronic Records Management systems (ERMS) in the public sector..

2.3.15 The requirements were specified in response to the e-government initiative and the need to meet FOI and DPA records management legislation. The first set of Requirements for ERMS was published in 1999, with an update in 2002[20].

2.3.16 This initiative led to the development of EDRM systems tailored for UK public sector records management needs and which, properly implemented, enable organisations to meet all the UK compliance requirements.

2.3.17 The TNA introduced a compliance-testing scheme and approved some 16 systems against the 1999 requirements. Against the revised 2002 requirements it approved around 10 products before testing ended in 2005.

2.3.18 The TNA has now joined forces with a European project to revise Europe's equivalent specification, MoReq[21], and has created a joint MoReq2 which was published earlier this year. This will also have a testing scheme in due course.

2.3.19 The TNA:2002 requirements focus on the records management and corporate aspects of electronic document management. They include support for a corporate business classification scheme, which subdivides records into classes, folders and parts, with retention schedules attached at any level. Central to TNA:2002 is the ability to declare documents as records, after which they are protected from change or deletion until their retention schedule expires. Search mechanisms, audit trails and reporting methods are also specified.

2.3.20 The Requirements specify the minimum metadata, which are now aligned with the e-GMS (see above). They make mandatory the use of the e-GMS Rights field to indicate protective marking and FOI and DPA disclosability.

2.3.21 The use of systems compliant with TNA:2002 or its successor MoReq2 is not compulsory, but is recommended for several reasons: -

- The use of classification and retention scheduling enables records to be maintained over time and deleted promptly when due for deletion.
- The use of standard metadata and classification methods will simplify the exchange of information between services and between authorities.
- Compliance with standards will also help ease the migration of records from current to future systems, complete with their metadata and audit trails. In the case of long record lifecycles, records will have to survive many such migration exercises.

2.3.22 Whilst TNA compliance is not a pre-requisite, neither is it sufficient. TNA:2002 focuses on records management requirements, with little mention of workflow, scanning or other EDRM technologies.

[20] Requirements for ERMS www.nationalarchives.gov.uk/documents/requirementsfinal.pdf

[21] Model Requirements for the Management of Electronic Records www.cornwell.co.uk/edrm/moreq.asp

Rather than mandate TNA approval any Statement of Requirements for an EDRM system should incorporate TNA requirements along with the Council’s own business requirements. The TNA rates each requirement as mandatory or desirable, but the Council can change the rating according to its own needs and priorities.

2.3.23 The TNA’s move to support MoReq2 will not make a major difference in the type of system that meets requirements. The systems that met TNA requirements are in the best position to comply in future with MoReq2.

2.3.24 Other countries have standards similar to TNA:2002 and MoReq e.g.

- DoD 5015 parts 2 and 4: the US standard ‘Design Criteria Standard for Electronic Records Management Software Applications’[22] published in 2002.
- DOMEA® Concept Requirement catalogue 2.0. The German standard published by the German Federal Government Co-ordination and Advisory Agency in 2005[23].

Other technical standards

2.3.25 There are several international standards relating to specific components or aspects of record keeping systems. Most technical standards are included in the National Archives Requirements for ERMS and need not be repeated here. The key ones to mention are:-

- **ISO 2788** is a standard for mono-lingual thesauri. Thesauri are used to control the contents of specified index fields in EDRM systems or Web Content Management systems, for example to select terms from IPSV (see e-GMS above) to populate the Subject metadata field. Compliance with ISO 2788 should be included in requirements when purchasing EDRM systems.
- **ISO 9000** is a set of standards for quality management systems, used in areas such as manufacturing, software development and professional services to ensure that processes are defined and outputs documented and cross-referenced. Compliance with ISO 9000 should be included in requirements when purchasing software or services.
- **ISO 8601** and the supporting document BSI DISC PD2000 specify the formats for recording date and time: e.g. YYYY-MM-DD or YYYY-MM-DDThh:mmTZD. Compliance with ISO 8601 should be included in requirements for purchasing EDRM systems.
- **ISO 17799:2000** is a Code of practice for information security management, now being replaced by the ISO 27000 series. The ability to support ISO 17799 should be specified as a requirement for any software procurement and should be implemented also in the configuration of that software.
- **ISO 27001 (2005)** is a British and international specification for information security management: replacing ISO 17799 and the old BS 7799-2 standard.
- **ISO 23081 2006** provides metadata standards.
- **BS 4783-1:1988** is a standard for storage, transportation and maintenance of media for use in data processing and information storage.

2.3.26 All are available to purchase through the BSI web site[24].

2.4 Principles for Information & Knowledge Management

2.4.1 Further to the above defined regulations and standards, the Council has through the Information and Knowledge Management Agenda, defined a set of principles which support delivery of the agenda. These Principles, are based on best-practice adopted from other public sector organizations and adhere to the regulations and standards outlined above.

[22] DoD 5015 http://www.dtic.mil/whs/directives/corres/html/501502std.htm

[23] DOMEA® http://www.kbst.bund.de

[24] BSI web site www.bsi-global.com

2.4.2 In this regard, the IKM Principles are standards that the Information Governance Framework must adhere to. The Principles are:

- **We share information appropriately and lawfully** – we will share our information and knowledge assets appropriately and in doing so handle them sensitively and in accordance with legal and regulatory requirements at all times.
- **Our information is open and** accessible – decision-makers at all levels within the Council will be able to get easy access to the information and knowledge they need at the time when they need it.
- **We use information ethically** – we will use information and knowledge in a way that ensures individuals' details are protected and only seen by the appropriate professionals in order to deliver the best possible service.
- **Our information is accurate and fit for purpose** – good quality information and knowledge assets are essential as evidence based decision-making is only as good as the quality of the underlying data and information.
- **We all have responsibilities for our information** – everyone within the Council has responsibilities for the information and knowledge assets they handle, whatever their level in the organisation.
- **We regard information as a Leeds City Council resource** – information and knowledge are Council resources that are not wholly 'owned' by any individual, team, service or directorate.
- **We value information as an asset to the Council** – in the same way that the Council looks after it's finances, people and capital assets. It will also look after it's information and knowledge assets in a more strategic way.
- **We have the skills and confidence to act according to these principles** – in order to uphold these principles we will identify and develop the skills across the Council to do so.

2.4.3 These eight principles aim to ensure that as an organisation the Council can manage, use and share its information and knowledge assets openly and safely.

INFORMATION & KNOWLEDGE MANAGEMENT

Leeds City Council
Information Governance Framework

Section 3

Information Governance Needs

INFORMATION GOVERNANCE NEEDS

3.0 Information Governance breaks down into a number of component parts, each of which must be addressed for compliance.

3.1 Access

3.1.1 Information should be available when, where and to whom it is needed. The principle of open access was laid down by the Freedom of Information Act and should be applied internally to the organisation as well as externally to subject access requests.

3.1.2 The main exemption to open access is personal information such as is found in Human Resources and Social Services. Access to sensitive personal data and documents should be restricted to the service or team that 'needs to know'.

3.1.3 Otherwise, open access can be the rule. Electronic information is more widely accessible than paper: it can be available to all who need it at the same time and from any location. Electronic information enables access to be provided for mobile and home working, for information sharing and joined-up working.

3.1.4 In implementing any software system an Access and Security Model is required to decide the user roles and access rights to be configured into the system. An identification of the information types and their FOI status is a good place to start. Joining up the access and security model into a corporate user directory will save end-user login time and IT support time.

3.1.5 The Council should have a 'clear desk' policy, both to ensure that records are made safe from inappropriate access and to reduce the fire risk.

3.2 Security

3.2.1 Security is of increasing importance, as leaks, losses and viruses become commonplace. Security is an issue for information in IT systems, information in transmission between systems and information in physical files.

3.2.2 Security is a broad term covering a number of categories: -

- ***Availability*** – the information must be available when needed. This is addressed by storage methods, software resilience, disaster recovery and preservation planning (see below).
- ***Authenticity*** – the recipient of information can be sure that the information was written by the sender. This is an issue for information in all forms.
- ***Confidentiality*** – only the intended and authorised recipients of information can have access. This is achieved by setting appropriate access restrictions to online information and by locks and passes barring access to physical files. Encryption may be required to protect confidential information in transmission (e.g. email) or on portable devices (e.g. laptops, PDAs and memory sticks).
- ***Integrity*** – the recipient can be sure that the information has not been changed at any time from that written by the author. This is built into electronic systems such as EDRM systems where active documents can be declared as 'records' after which they cannot be changed. There is less integrity in documents on shared drives: they can very easily be moved, deleted or overwritten.
- ***Non-repudiation*** – this is a variation on authenticity: the sender cannot later deny having written the information, and the recipient cannot later deny having received it. Signatures are used with paper documents for this purpose, although they do not necessarily provide strong evidential weight. For electronic documents of high legal value, such as contracts and deeds, digital certificate techniques may be needed, involving PKI (Public Key Infrastructure) technology.

3.2.3 There are ISO standards covering the security of information in both electronic and physical form: ISO 17799[1] and ISO 27000. (See above).

3.3 Retention

3.3.1 Setting retention and disposal schedules is important in order to avoid breaching the Data Protection Act for personal information, and also to restrict the growing volumes of paper and electronic documents and datasets.

3.3.2 A retention schedule is comprised of two factors: an event and a time period. The event might be a calendar event, such as the end of the financial year, or an external event, such as the termination of a contract. The time period can vary from 1 year (disciplinary warning) to 75 years (e.g. looked-after children) to indefinite retention (e.g. the Planning Register). Sometimes the 'retention clock' starts ticking from the date the document was created, sometime from the date the folder it resides in was closed. Sometimes, during an enquiry or access request, the information is put 'on hold' and a different retention schedule might be picked up when the information is released from hold.

3.3.3 The Records Management Society has developed a set of 'Retention Guidelines for Local Authorities'[2]. These are based on statutory grounds and common practice. However, they are only guidelines. Some Council services may have retention needs beyond the norm. Where current practice differs from the Guidelines the differences are worth investigation.

3.3.4 Often forgotten is the need to limit retention in data systems, particularly databases containing personal information. The ability to schedule the deletion of data is a requirement that should be written into specifications for all such systems.

3.4 Formats

3.4.1 Electronic file formats are short-lived entities. Each generation of software supersedes its predecessor, and while backwards compatibility is usually maintained for a generation or two, in 10 or 15 years today's Word document or CAD file will not be readable on the desktop software of the time.

3.4.2 There are methods of coping with format obsolescence: format conversion and software emulation. Format conversion requires the migration of documents from one format to another – maybe an earlier Word version to a later one, or a Word document to PDF. This necessitates a constant technology watch, so that formats can be converted before their software is lost.

3.4.3 Preservation planning favours the use of long-term formats such as PDF, TXT, TIFF, HTML or XML. Emails should be saved in shared drives (or EDRM) in HTML or TXT formats. For documents that require reuse the best method may be to create duplicate formats, for example PDF for longevity and Word for reusability.

3.4.4 Software emulation is another option. There are viewers already for obsolete formats such as WordPerfect or WordStar and there is hope that one day an all-purpose emulator will let us view, if not reuse, our out-of-date file formats.

3.5 Media

3.5.1 Off-line storage media such as CDs and tapes are not suitable for long-term retention.

3.5.2 Media suppliers often quote long lifecycles for their products. These are largely irrelevant. The technology of storage media often has a shorter lifespan than the media it uses.

3.5.3 New computers are no longer issued with drives for 3.5 inch disks, and we have no way of reading their predecessors the 5.25 inch and 8 inch disk. CD drives are being replaced with DVDs. Magneto-

[1] BS ISO/IEC 17799:2005 Information technology. Security techniques. Code of practice for information security management. From www.bsi-global.com

[2] Retention Guidelines for Local Authorities www.rms-gb.org.uk/sigs/local-government/resources

optical disks have passed through several generations each with different size and capacity as have magnetic tapes. The media we use today will not be readable in 10 or 20 years time.

3.5.4 Fortunately the cost of online storage has reduced to the point where offline storage media are not needed. Growing storage volumes are a problem but are more an issue of backup times than disk space costs.

3.5.5 If near-line or off-line storage is required for any reason, then fast and proven export methods are a pre-requirement of any implementation.

3.6 Preservation

3.6.1 Preservation of information is an issue of growing concern as more and more information goes electronic.

3.6.2 Paper files, given protection from fire and flood, are likely to last many decades before they become illegible. The use of archive (non-acidic) paper and plastic tags can extend their life even longer.

3.6.3 For electronic information, preservation is more complex and is an issue to which there are no easy solutions yet. In essence, electronic preservation is a matter of overcoming the obsolescence built into formats and media.

3.6.4 Any software implementation project must include preservation planning, to ensure that information is not locked into obsolescent formats and media. Preservation planning must ensure the use of long-term formats and on-line or fast-access near-line media. It must include a ‘technology watch’ to identify documents in obsolescent formats and provide the means of carrying out bulk migration or conversion on the documents identified.

3.6.5 EDRM provides the best hope for document preservation. The metadata in EDRM systems enables records managers to identify document types and formats. The records management functionality enables them to carry out bulk movement or conversion on the obsolescent document types found.

3.6.6 Each Council service should carry out an information audit to find out (among other objectives) what information is currently stored in CDs, tapes and other offline media, so that plans can be put in place to upload their contents to online storage.

3.6.7 The National Archives is leading on preservation methods and has issued guidance on its website[3].

3.7 Databases

3.7.1 Data in databases is not too hard to preserve, as most databases are held online. However, the software application and the supporting database and operating system will all become obsolete over time and data will need migration every 7 years or so to new databases, new operating systems and new applications.

3.7.2 There are two risks that are sometimes overlooked. It is tempting to leave old data in the current application while starting afresh with its successor. This is not a sustainable solution. The superseded database will not be supportable for long and when the hardware fails it may be too late to extract the data.

3.7.3 The other risk is archiving. Archiving methods vary greatly but if data is archived to off-line media then obsolescence is a high risk. If archiving is to on-line storage there is still the danger that it might not be reloadable after changes to the live database.

3.8 Data Quality

3.8.1 Data quality is an issue for data in databases and metadata in EDRM systems. The criteria for data quality are completeness, validity, consistency, timeliness and accuracy.

[3] National Archives preservation guidance www.nationalarchives.gov.uk/preservation/advice/digital.htm

3.8.2 This last, accuracy, is one of the common weaknesses in database applications. Accuracy can be improved by: -

- Validating data entry: by look-up lists, address matching etc.
- Automating data entry: from electronic forms
- Automating the exchange of data: by integrating systems.

3.8.3 Consistency is required not only within databases but between them. Standardised data will enable the Council to exchange data between services, join up front and back offices and collate information into data warehouses. In many cases data is a local part of a national initiative (e.g. the National Land and Property Gazetteer) that requires compliance with an external standard data model.

3.8.4 Timeliness is achieved by updating systems whenever information is received or data changed. Using a single central source for people and property data, integrated into line of business systems, will assist with accuracy and timeliness.

3.8.5 Data should conform wherever applicable to the Government Data Standards Catalogue (GDSC)[4].

3.8.6 GDSC standards include the property references (BS7666)

- Names and addresses
- Person identifiers
- Dates and times.

3.8.7 For the metadata in an EDRM system the e-Government Metadata Standards prescribes the standard data fields and GDSC, along with IPSV (see Technical Standards above), prescribes much of the contents. There is a metadata standard ISO 23081 2006[5], which will provide assistance in setting up Leeds-specific or service-specific metadata.

3.9 Emails

3.9.1 Email folders are not a suitable place to keep records. They create separate ‘silos’ of information available only to one member of staff. They are not shared for joined-up working, not available to FOI and DPA searches and difficult to hand over to successors in post.

3.9.2 All emails of record, i.e. not transient emails and circulated memos, should be saved onto shared drives or an EDRM system.

3.9.3 It is easier to save emails to an EDRM system. The system automatically captures the subject, sender, recipient, data and time. It captures the attachment as well as the message and links them together. Internal emails do not need attachments, but (if everyone is on the same EDRM system) can use a URL link. That reduces the volume of attachment traffic and avoids the version control problems that happen when multiple versions of the same documents are emailed repeatedly to long distribution lists.

3.9.4 Email protocols are also required to prescribe the use of meaningful subject lines and text, to clearly distinguish emails to be actioned from emails for information only and to prevent long email chains. Instructions on the use of out-of-office messages will be required.

3.10 Legal Admissibility

3.10.1 Many Council documents might be required in court and it is not possible to accurately predict which ones. It is possible however to estimate the importance of document types and the risks attached to not finding them or not keeping them in an admissible form.

3.10.2 Legal admissibility is a matter of evidential weight. The medium the record is held on (electronic, paper or other) does not necessarily contribute to its evidential weight but the security and audit trail

[4] Government Data Standards Catalogue www.govtalk.gov.uk/gdsc/html/frames

[5] BS ISO 23081-1:2006 available from http://www.bsi-global.com

around the item does. There is a BSI Code of Practice for Legal Admissibility and Evidential Weight, released in 1999 as PD0008 and revised in 2004 as BIP 0008[6].

3.10.3 The Lord Chancellor's Code of Practice under Section 46 of the Freedom of Information Act also recommends BIP 0008, especially for those records likely to be required as evidence.

3.10.4 The code is divided into five parts:

- Representation of information
- Duty of care
- Business procedures and processes
- Enabling technologies
- Audit trails

3.10.5 BIP 0008 requires system features such as complex security and document-level audit trails which all EDRM systems can provide.

3.10.6 It also requires the writing of policies and procedures, especially around scanning, and the training of all staff to ensure that these procedures are followed. Quality control procedures and training are easier to implement where scanning is centralised into a dedicated team, rather than distributed among a large number of local administrative staff.

3.10.7 An Information Audit can be used (among other objectives) to identify documents requiring legal admissibility and ensure that they are either retained on paper or captured into an EDRM system using BIP 0008-compliant procedures.

3.11 Information Sharing

3.11.1 The Council interacts with the public, with commercial partners, with other councils, with schools, with the health service, with police and fire authorities, with the department for Communities and Local Government, with contractors and consultants and with community organisations.

3.11.2 Services require information sharing protocols, to decide what information can be shared and with whom. Within the rules of the protocol, Individual Sharing Agreements are required to cover the sharing of information between any two (or more) parties.

3.11.3 If information is passed to commercial organisations, then it must be done so fairly and in accordance with the Re-use of Public Sector Regulations (see above).

3.11.4 Social Services must have information sharing protocols for the case file information shared with schools, police, other authorities and the health service. See the 'Leeds Interagency Protocol for Sharing Information' on the intranet.

3.11.5 A template for Information Sharing Protocols can be found on the Home Office website[7].

3.12 Intellectual Property Rights

3.12.1 Intellectual property laws cover copyright, designs, patents and trade marks. The law most likely to be breached in local authorities is copyright. Copyright law[8] protects material such as literature, art, music, sound recordings, films and broadcasts.

3.12.2 Copyright is automatically conferred. The author or creator does not have to apply for it and the material does not have to state it.

3.12.3 Copyright applies to any medium. You must not reproduce copyright protected work in any medium without permission. This includes photocopying protected documents, publishing photographs on the internet, downloading documents from the internet or putting scanned newspaper articles online.

[6] BIP 0008:2004 Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically www.bsi-global.com/en/Standards-and-Publications/Industry-Sectors/ICT/ICT-standards/BIP-0008-1/

[7] Home Office Crime Reduction Information Sharing web pages www.crimereduction.gov.uk/infosharing/infosharing00.htm

[8] Copyright, Designs and Patents Act 1988 www.opsi.gov.uk/acts/acts1988/Ukpga_19880048_en_1.htm

3.12.4 There is an assumption that publishing a document on the internet automatically waivers copyright. That is not the case. If a document, photograph or piece of music on the internet is not clearly intended for free public use, then permission must be sought.

3.12.5 The greater dangers to the Council are in the reproduction of purchased reference material, such as books, CDs, photographs or newspaper articles. These should not be copied or put online unless the Council owns the copyright or has permission to use the material.

3.12.6 For material created for the Council, such as photographs and designs, the owner must be decided (originator or Council) and their rights protected. In EDRM systems there are metadata flags to store IPR information.

3.13 Information Content

3.13.1 So far the issues in Information Governance have been to do with the management of information. Also important is the need to improve the content of information.

3.13.2 There are various ways to improve content: -

- Set up Word templates for standard documents such as meeting papers, management reports, memos, letters and faxes to ensure consistency of structure and content. Templates should prescribe the structure of the document, the titling, headers and footers and version numbering. Templates used in conjunction with EDRM systems can pass the header information into EDRM metadata.
- Set up version control standards, prescribing the use of version control for all changed documents and the format of the version numbering. EDRM helps here by controlling versions and ensuring that only the latest version is immediately visible.
- Draw up an email protocol to prescribe the format and content of emails (see Emails above) to ensure that the content and particularly the subject line are meaningful, to clearly identify emails for action and emails for information only and to avoid the creation of long email chains.
- Set up naming conventions for file titling in shared drives to include title, date, author and document type. In EDRM systems, this will be less onerous as the data, author, title and document type will be captured in the metadata.

INFORMATION & KNOWLEDGE MANAGEMENT

DRAFT

Leeds City Council
Information Governance Framework

Section 4

The Information Governance Framework

THE INFORMATION GOVERNANCE FRAMEWORK

4.1 The Framework

4.1.1 The Information Governance Framework provides the intellectual architecture which governs how Leeds City Council captures, creates, accesses, secures, manages and shares its information both internally and externally.

4.1.2 The Leeds Framework has been developed based on best practice models adopted nationally. These include the NHS Information Governance Toolkit and the draft Local Government Information Governance Toolkit. Further development of these models within the context of Leeds has also be aided through a similar exercise being conducted on a West Yorkshire basis through the West Yorkshire Information Management Forum.

4.1.3 The Framework is structured around 6 areas of Information Governance as follows:

- Information Governance Management
- Records Management
- Information Compliance
- Information Security
- Data Quality & Assurance
- Information Sharing

4.1.4 Details on each of the six areas are outlined below. For each, a rationale as to why it is a key competent of the Framework is provided, this is followed by the objectives that are sought through delivery of the Framework and the supporting policies and procedures that will enable the framework to become real within the organisation.

4.2 Information Governance Management

Rationale for Information Governance Management

4.2.1 This covers the management of information governance at a corporate, managerial and operational level across the organisation. It is one of the fundamental component of the Framework as it will provide the necessary ownership and advocacy functions that can be used to ensure the promotion, development and implementation of the appropriate information governance infrastructure is delivered across the organisation.

Objectives for Information Governance Management

4.2.2 The following outline the required objectives to ensure delivery of an appropriate Information Governance Management function:

REF	Objective
IMG 1	Leeds City Council has a formally recognised corporate Information Governance Group with agreed Terms of Reference. The Group should sit in an appropriate place within the broader Corporate Governance arrangements
IMG 2	The Information Governance Group has access to the necessary expertise across all six areas of the Framework
IMG 3	Leeds City Council has an approved Information Governance Framework
IMG 4	Leeds City Council has an approved Information Governance Statement
IMG 5	Leeds City Council has an approved Information Management Policy

IMG 6	There are clearly defined corporate and managerial stewardship responsibilities for information governance across Leeds City Council.
IMG 7	Leeds City Council has an approved corporate information governance improvement plan that is managed and monitored by the information governance group
IMG 8	An established review process exists to maintain the currency of the Information Governance Framework within the Council.
IMG 9	Staff induction procedures across the Council effectively raise the awareness of information governance and outline individual responsibilities contained therein.
IMG 10	Core information governance competencies are built into all Job Descriptions and an appropriate Training and Development programme established to facilitate their delivery.

Policies and Procedures in support of Information Governance Management

4.2.3 The following policies and procedures are required within Leeds City Council to ensure delivery of the 10 Information Governance Management objectives outlined above.

- Corporate Information Governance Group Terms of Reference
- Leeds City Council Information Governance Framework
- Information Governance Framework – Policy Review Procedure
- Leeds City Council Information Governance Statement
- Leeds City Council Information Management Policy
- Corporate Information Governance Improvement Plan (3 yearly)
- Information Governance Stewardship and Accountability Framework
- Information Governance Skills and Competency Framework
- Information Governance Workforce Development Plan
- Information Governance Training and Development Programme.
- Information Governance Induction procedure
- Information Governance – staff guidance manual

4.3 Records Management

Rationale for Records Management

4.3.1 Records Management covers the process of creating, describing, using, storing, archiving and disposing of organisational records according to a defined set of standards (usually adherence to ISO 15489). It is one of the fundamental components of the Information Governance Framework as it ensures the Council's record sets enable adherence to compliance rules and statutory access requirements as well as protecting an organisation's corporate memory for re-use.

Objectives for Records Management

4.3.2 The following outline the required objectives to ensure delivery of an appropriate Records Management function:

REF	Objective
RM 1	Leeds City Council has an agreed ISO 15489 compliant Records Management policy.
RM 2	Leeds City Council has agreed and implemented a Business Classification Scheme which incorporates security (access and permission) rules.
RM 3	Leeds City Council has agreed and implemented a Record Retention and Disposition Policy

RM 4	Leeds City Council has agreed and embedded corporate records management metadata standards which meet national standards as a minimum.
RM 5	Leeds City Council has agreed and implemented a Version Control Policy
RM 6	Leeds City Council has agreed and implemented a Security & Access Policy
RM 7	An established review procedure exists to protect the currency of the Records Management Policy within the Council
RM 8	Leeds City Council has documented procedures to ensure delivery of the Records Management policy. As a minimum, these should cover: • Storage and Handling • Preservation and Future-proofing • Audit and Tracking • Business Continuity • Legal Admissibility • Access and Retrieval
RM 9	Leeds City Council has deployed appropriate systems to manage the organisation's records in line with the corporate Records Management policy.
RM 10	A Controlled Business Vocabulary (or taxonomy) is developed and embedded within electronic document and records management to maintain the link between business usability and the Business Classification Scheme
RM 11	Leeds City Council has a Records Management function that has the required capacity to develop, implement and embed the Records Management policy across the organisation
RM 12	Core Records Management competencies are built into appropriate Job Descriptions and a suitable Training and Development programme established to facilitate their delivery.

Policies and Procedures in support of Records Management

4.3.3 Further to those established for Information Governance Management, the following policies and procedures are required within Leeds City Council to ensure delivery of the 12 Records Management objectives outlined above.

- Corporate Records Management Policy
- Records Creation Policy
- Records Capture Policy
- Business Classification Scheme
- Records Retention and Disposition Policy
- Records Security and Access Policy
- Storage and Handling Procedure
- Preservation and Future-Proofing Procedure
- Audit and Tracking Procedure
- Business Continuity Procedure
- Legal Admissibility Procedure
- Access and Retrieval Procedure
- Controlled Business Vocabulary

- Physical Preservation of Records

4.4 Information Compliance

Rationale for Information Compliance

4.4.1 Compliance covers the legal framework and the standards that need to be established to ensure information management is within the law. The Council manages and processes large volumes of confidential and sensitive information and knowledge about people. It must deal with this lawfully and ethically. Failure to do so could endanger individuals and can also increase risk, loss of reputation and litigation. The key legislation it must comply with includes the Data Protection Act, the Freedom of Information Act, the Human Rights Act, the Environmental Information Regulations and Re-Use of Public Sector Information Regulations.

Objectives for Information Compliance

4.4.1 The following outline the required objectives to ensure delivery of an appropriate Information Compliance function:

REF	Objective
	INFORMATION RIGHTS (Includes DPA/FOI/EIR/RIPA/PIR etc)
IC 1	Leeds City Council has an approved and monitored Access to Information policy which sets out corporate procedures, roles and responsibilities.
IC 2	Directorates will make sure that they have appointed dedicated officers who are responsible for managing and processing Access to Information requests. All such officers will have access to regular training on information rights legislation.
IC 3	Leeds City Council has a corporate framework for evaluating the public interest test for disclosing information through Access to Information requests in a consistent and transparent manner.
IC 4	All staff employed by Leeds City Council are aware and trained in the various rights of access to information and how these can be exercised inclusively.
IC 5	The public are made aware of their information rights and how to exercise them.
IC 6	Staff ensure that information is provided in the most appropriately accessible format within statutory timescales.
IC 7	Leeds City Council has an effective mechanism in place to consider appeals to withhold information under both FOI and EIR requests.
IC 8	Leeds City Council has a standard licence agreement to issue to external parties requesting information for further use under the Re-Use of Public Sector Information Regulations. The Information and Knowledge Management Team will maintain a register of information assets and audit compliance.
	STANDARDS
IC 8	Personal information is processed in a manner compliant with the Data Protection Principles.
IC 9	Intellectual property rights (e.g. copyright) are observed.
IC 10	All staff are made aware of and abide by their obligations under the Common Law Duty of Confidentiality.

Policies and procedures in Support of Information Compliance

4.4.2 Further to those established for Information Governance Management, the following policies and procedures are required within Leeds City Council to ensure delivery of the 10 Information Compliance objectives outlined above.

- Data Protection Policy
- Staff guidance to Data Protection

- Guidance and procedure to disclosures
- Guidance and procedure to subject access requests
- Public guide to subject access requests
- Freedom of Information Policy
- Staff guidance to Freedom of Information
- Guidance and procedure to disclosure and exempted information
- Procurement guidance
- FOI guidance for Members
- Guidance on Privacy Impact Assessments
- Environmental Information Regulations Policy
- Staff guidance to EIR
- Policy document on the Re-Use of Public Sector Information Regulations
- Regulation of Investigatory Powers Policy
- Staff guidance on RIPA
- Covert Surveillance Code of Practice

4.5 Information Security

Rationale for Information Security

4.5.1 Information security covers the policies and procedures in place to protect information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. Adherence to the principles of ISO 270001 will deliver information security compliance. It is one of the fundamental components of the Information Governance Framework as it will ensure the Council is able to protect the confidentiality, integrity and availability of information within the organisation and when sharing with partners.

Objectives for Information Security

4.5.2 The following outline the required objectives to ensure delivery of an appropriate Information Security function:

REF	Objective
IS 1	There is an Information Security Policy in place based on ISO 270001
IS 2	Roles and responsibilities for adherence to the policy are clearly defined and an appropriate training and development programme is in place.
IS 3	There is an inventory of information assets, as defined in ISO 270001, supported by a Protective Marking Scheme
IS 4	Access control is in line with the security policy and the need for information dissemination and authorisation
IS 5	There is a Risk Management Framework in place and information security risks are incorporated.
IS 6	Security requirements are included in formal system acquisition, development and maintenance procedures
IS 7	Formal procedures are in place to avoid breaches of the law, statutory, regulatory or contractual obligations, and of any security requirements.
IS 8	There are procedures to report information security incidents and weaknesses and to escalate action on dealing with these. Staff are made fully aware of the procedures.
IS 9	There is a business continuity management process designed to limit the impact of, and recover from the loss of information assets.

IS 10	Operation procedures for the use of equipment is available to all users who need them. The procedures are documented and maintained.
IS 11	All changes to information processes are planned and implementation is effectively managed.
IS 12	There are controls in place for managing Third Party agreements
IS 13	There are appropriate physical security controls in place to protect information assets
IS 14	Networks are adequately managed and controlled to protect them from threats. Security is provided for the systems and applications using the network
IS 15	Information Security Management procedures are independently reviewed

Policies and Procedures in support of Information Security

4.5.3 Further to those established for Information Governance Management, the following policies and procedures are required within Leeds City Council to ensure delivery of the 15 Information Security objectives outlined above.

- Information Security Policy
- Information Security Manual/Staff Guidance
- Access and Permissions Security Policy
- Security of Third Party Access Policy
- E-Mail Code of Practice
- Internet Usage Policy
- Information Security Classification
- Anti-Virus Policy
- Code of Practice for Information Security Management
- Code of Conduct for the use of Software
- Code of Conduct for the use of IT Systems
- Code of Conduct for Mobile and Remote Working
- Code of Conduct for Systems Administrators

4.6 Data Quality and Assurance

Rationale for Data Quality Assurance

4.6.1 This set of requirements covers the need to ensure the quality, accuracy, currency and other characteristics of information products. It is one of the fundamental components of the Information Governance Framework as both staff and customers will be able to trust the validity and authority of information sources, and have confidence that it is up-to-date and accurate. It is important that the Council is able to measure the level of quality of its information resources and ensure they comply with relevant standards.

Objectives for Data Quality Assurance

4.6.2 The following outline the required objectives to ensure delivery of an appropriate Data Quality Assurance function.

REF	Objective
DQA 1	Leeds City Council has an agreed Data Quality Strategy and Policy.
DQA 2	Leeds City Council has a designated Data Quality Champion at executive level.

DQA 3	There are designated Data Stewardship roles with specific responsibility for data quality across the Council.
DQA 4	Data quality competencies are built into all job descriptions. Where colleagues have specific responsibilities around data, suitable training and development programmes are developed.
DQA 5	There are business continuity plans in place for all systems.
DQA 6	Minimum standards are set for the quality of data being shared with external organisations and there are standards for data quality applied to data being provided to the Council.
DQA 7	There are documented procedures and processes in place governing the capturing, recording and handling of data.
DQA 8	There are documented procedures for data collection activities and these procedures are monitored.
DQA 9	Data quality checks are incorporated into processes and procedures around the handling of data.
DQA 10	Leeds City Council has a set of metrics which can be used to assess the quality of data in key systems.
DQA 11	There are documented standards for the Council's data items to provide consistency across the systems and in reporting. Where national standards around data are not available local standards will be agreed.
DQA 12	Leeds City Council has a framework to enable the continuous assessment and regular monitoring of data quality.
DQA 13	Leeds City Council uses the appropriate technologies to support its data quality improvement activities.

Policies & Procedures and in support of Data Quality Assurance

4.6.3 Further to those established for Information Governance Management, the following policies and procedures are required within Leeds City Council to ensure delivery of the 13 Data Quality Assurance objectives outlined above:

- Data Quality Strategy
- Data Governance Strategy
- Data Quality Policy
- Leeds City Council Data Standards
- Data Sharing Policy
- Master Data Management Strategy
- Data Integration Policy
- Records Retention and Disposition Policy
- Business Continuity Procedure
- Information Security Policy
- Access and Permissions Security Policy
- Leeds City Council Information Sharing Protocol

4.7 Information Sharing

Rationale for Information Sharing

4.7.1 Information sharing covers the proper governance of information sharing practice across the Council; it is an essential component given that it deals with business activities involving the potential for sharing personal information about our customers, staff and other stakeholders. Ensuring that our practice is of the highest standard, meeting with regulatory mechanisms such as the Data Protection and Human Rights Acts together with the Common Law Duty of Confidentiality, is essential in order to imbue confidence amongst those whose personal information is involved in such business processes.

Objectives for Information Sharing

4.7.2 The following outline the required objectives to ensure delivery of an appropriate Information Sharing function.

REF	Objective
ISG1	There is an agreed information sharing protocol in place setting out principles, operational procedures and key legislative considerations together with practical user guidance on the following: • Obtaining consent to share (including establishing fitness to consent); • Sharing without consent; • Access and security purposes; • Use of additional purposes; • Determining the “need to know”; • Completion of template information sharing agreements; and • Application of key legislative considerations.
ISG 2	Leeds City Council has a standardised, documented approach to information sharing in place and full use is being made of template guidance.
ISG 3	All information sharing agreements are completed in full detail setting out in particular the legal justification for each sharing exercise.
ISG 4	Each Directorate has a nominated trained practitioner available to give guidance on key legal issues in relation to justification for information sharing.
ISG 5	Each Directorate has an audit log of its information sharing agreements, recording sufficient detail of each exchange with particular regard to purpose, justification, nominated contacts and review period.
ISG 6	All information sharing agreements are centrally logged with the Information and Knowledge Management Team.
ISG 7	All information sharing agreements are reviewed in the month prior to expiration to ensure continued validity.
ISG 8	A mechanism for reporting breaches of the protocol and/or specific agreements is documented, agreed and in place for both internal and external parties.
ISG 9	A mechanism for monitoring the operation and effectiveness of the protocol is documented, agreed and in place.
ISG 10	Directorates will, on request, provide assurances that agreed procedures and practice are being followed.
ISG 11	Operation of the Information Sharing Protocol is included as a standing item on the agenda of the Information Governance Group in order to address on a regular basis any issues that may arise.
ISG 12	All nominated practitioners are properly trained and equipped in order to provide effective advice and guidance.

ISG 13	A training package is developed and in place for all staff involved in day to day information sharing.
ISG 14	An outline of the protocol and operational procedures is included in the staff induction process.

Policies & Procedures in support of Information Sharing

4.7.3 Further to those established for Information Governance Management, the following policies and procedures are required within Leeds City Council to ensure delivery of the 14 Information Sharing objectives outlined above:

- Leeds City Council Information Sharing Protocol
- Information Sharing Protocol – review procedure
- Corporate Operational Procedures for Sharing Information; (comprising):
  - *Procedures for sharing information*
  - *Access and security procedures*
  - *Procedure for management and review of the protocol*
- Corporate Information Sharing Agreement Template
- Procedure for logging information sharing agreements within the organisation and Directorates
- Breach Rectification Procedure
- Training for practitioners on legal considerations
- Guidance manual for operational staff

INFORMATION & KNOWLEDGE MANAGEMENT

Leeds City Council
Information Governance Framework

Section 5

Support Arrangements

INFORMATION & KNOWLEDGE MANAGEMENT

Leeds CITY COUNCIL

SUPPORT ARRANGEMENTS

5.1 SKILLS AND COMPETENCY FRAMEWORK

INFORMATION & KNOWLEDGE MANAGEMENT

Leeds CITY COUNCIL

IKM Skills and Competency Framework

October 2008

INFORMATION & KNOWLEDGE MANAGEMENT

Leeds CITY COUNCIL

1.0 BACKGROUND

1.1 The Council can be described as being information rich but intelligence poor. Whilst we may be suffering from 'information glut' in terms of the volume of data and information we hold, we currently do not leverage this data and information and exploit it for the benefit of the Council and its customers. Consider the amount of hard copy records the Council holds; the information stored in electronic documents; databases; spreadsheets; emails and the knowledge and information locked away in people's heads. We currently don't have any overall structure to this information, any over-arching policy that states how this information should be managed and stored, when it should be disposed of, who is responsible for it, how up-to-date it is etc. This clearly impacts our organisational effectiveness.

1.2 The Gartner Group (Global IT Consultancy), talk about Information being the 4th Estate. In the same way that organisations look after their finances, people and capital assets they should also look after their information. Information poorly managed or not managed at all becomes a liability to an organisation.

1.3 In order to maximise the use of data and information as an organisation, we need to 'look after' it in a much more strategic way. This means, developing an appropriate Information Governance Framework with corporate policies that are, over time rolled out throughout the organisation. In order to do this effectively, the organisation needs to have in place an appropriate Information Management Structure that is built around people with the right skills and competencies.

1.4 In managing our information more effectively our greatest challenge lies in the cultural shift we need to make towards recognising that the information created and used within the organisation is not owned by any one individual, team, service or department. It is an asset of the organisation and should be used as such. Consequently, we need to move towards greater openness and transparency in the way that we share this knowledge and information. In this way we will over time, be able to leverage the value from this information and create a collaborative and learning environment. This is fundamental to the delivery of the Information and Knowledge Management (IKM) agenda within the Council.

2.0 AN ORGANISATIONAL MODEL FOR IKM IN LEEDS

2.1 The Council Change programme presents an opportunity to fundamentally address the issue of how the Council will ensure Information Management becomes integral to a 'fit for the future' organisation; moving away from being 'information rich' to being 'intelligence rich.'

2.2 The proposed model for making this happen is to establish an IKM Competency Centre, which is an adaptation of a best practice model. The idea of a Competency Centre is that it brings together people from a variety of disciplines and with a range of skills to work on a common agenda.

2.3 An IKM Competency Centre is Business led rather than ICT led and will draw on the ICT specialist skills required to ensure that the necessary technical infrastructures and technical deployments are delivered.

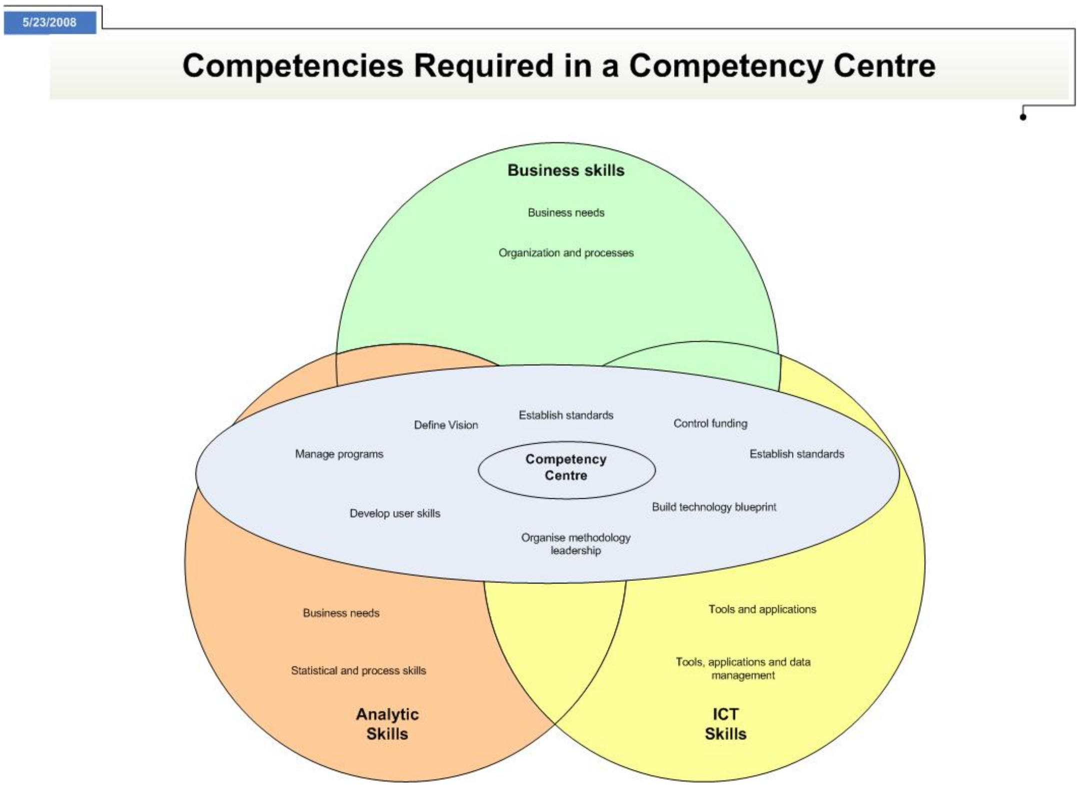
2.4 Whilst there are a number of different Competency Centre Models to fit a wide range of organisations, the model most suited to Leeds, particularly in light of the change programme is that of the Distributed Competency Centre. This would see a core (virtual) team within the Central and Corporate function with teams in each of the strategic directorates with direct links into the core team.

2.5 Alongside the formal structures of the Competency Centre are a number of connected roles that could be described as quasi members of the Competency Centre. These roles would include:

- Members of the Corporate Leadership Team particularly the Information and Knowledge Management Champion.
- Information Management specialists working across a range of disciplines (within business areas and ICT)
- Stewards - stewardship responsibilities are discussed below.

2.6 This distributed model would allow both IKM strategic policy development (driven by the core team) and the roll-out of policy and practice (driven by the distributed teams). In this regard the distributed teams would fulfil information management 'expert roles'.

2.7 The diagram set out below illustrates how Business Skills, ICT Skills and Analytical Skills should be brought together into a Competency Centre. The integration of these specialisms mean that there is a coherence to IKM strategy and policy development as well as decisions about priorities and end-to-end delivery. Gartner state that, "*A Competency Centre that is not created with a balance of authority and power between business, technology and analytics members will not achieve its maximum potential*." They also identify the involvement of users as crucial to the successful deployment and delivery of Information and Knowledge Management initiatives.



5/23/2008

Competencies Required in a Competency Centre

2.8 Points to note about the model:

- The Core Competency Centre should have a balance in skill sets and be empowered to deliver the Information and Knowledge Management Agenda
- The Competency Centre should report to a main business executive.
- The Competency Centre needs to have a stable core and be flexible enough to adapt and respond to meet the priorities of the organisation.

2.9 The benefits that a distributed IKM Competency Centre can bring are as follows:

- There is demonstrable evidence that the Council takes IKM seriously (the 4th Estate);
- There is a dedicated resource to improving the Council's approach to IKM at both a strategic and operational level;
- There is a dedicated resource for IKM strategy and policy development that meets the needs of the 'fit for the future' organisation by being adaptive to emerging agendas;
- There is clarity regarding the types of skills and competencies that are required to deliver the agenda;
- There is an identifiable resource within each of the Strategic Directorates with the skills and competencies to provide support, guidance, expertise, training and stewardship for functions and services;
- Skills and competencies within the organisation can be organised so as to improve capacity and enhance the corporate resource.

2.10 Given the above, the roles and responsibilities of a distributed Competency Centre can be articulated as follows:

The core team

- The core team would be located within the Head Office;
- The team would be responsible for the development of strategy and policy in relation to IKM;
- The team would have responsibility for Information Management Stewardship at a strategic level;
- The team would facilitate and support deployment of technical solutions in relation to Enterprise Content Management, Business Intelligence and Collaboration/Learning;
- The team would develop the underlying Information Governance framework required to underpin any technical deployments;
- The team would be responsible for setting out the strategies and policies to improve data quality within the Authority;
- The team would have corporate capacity in the areas mentioned in 2.7 above;
- The Core team would work closely with colleagues within the distributed teams to roll out policy and practice and provide support and guidance;

The distributed teams

- The distributed teams would be located within each of the Strategic Directorates.
- They would be responsible for rolling our corporate IKM policy, practice and technology within the functional / service areas they work with.
- They would be responsible for Stewardship in relation to Information Governance.
- They would provide a feedback loop into the core team to ensure the corporate IKM framework continued to meet the needs of the Strategic Directorate's agenda.
- The teams would have capacity that would also include the following areas;
    - Improving Data Quality
    - Freedom of Information
    - Data Protection
    - Records management, including, maintenance of retention and disposition policies and classification schemes for file plans.

2.11 As stated above, in order for the Council to start to recognise the value of its information and knowledge there are a number of building blocks that need to be put in place.

- Firstly, that IKM is recognised as fundamental to the Council achieving its ambitions for the future.

- Secondly, that the Council puts in place a structure that ensures that IKM is placed appropriately within the organisation; with both strategic policy direction and practical deployment; and

- Thirdly, that the Council identifies the skills and competencies required to deliver the agenda, brings them together where they already exist and develops / recruits them where they don't.

2.12 It is obviously the case that relevant IKM skills and competencies already exist within the Council with colleagues whose roles and responsibilities reflect this. However it is also the case that these roles and responsibilities are in a number of areas mere 'add-ons' to existing roles, with little attention paid to the knowledge, skills and competencies required to be fully effective in the role.

2.13 Given this, what follows outlines the 'types' of skills and competencies required in the 'fit for the future' Council to effectively manage our information and knowledge assets.

3.0 INFORMATION AND KNOWLEDGE MANAGEMENT SKILLS AND COMPETENCIES

3.1 To effectively deliver the IKM agenda, specific skills and competencies are required. These should be viewed as skills and competencies not just for the present (i.e. to address an immediate issue), but thought about more fundamentally as skill-sets to develop/recruit to both now and over time in order that the Council is equipped to fully realise the strategic value that exists within its information and knowledge.

3.2 Whilst some of these skills and competencies will have to be developed/recruited into the organisation, some will need to be re-invigorated for the 21st Century; especially those skill-sets that were allowed to diminish within the organisation with the onset of Desktop PCs (e.g. Document and Records Management skills and competencies).

3.3 A range of skills and competencies will be required depending on the different role and responsibilities that need to exist. For example some roles will require highly specialist skills (e.g. data integration); whereas other roles will require less specialised and more generalist skills across a wider range of IKM issues (e.g. strategic policy development). There will also be roles that demand versatility; for example, having the skills and competencies to move between generalist and specialist roles dependent on the projects / initiatives being worked on. It is intended (as indicated in the matrix attached at appendix 1) that these levels are indicated by the range of one to five. One, being a basic awareness level and five being a highly specialised level.

3.4 Furthermore to the above, there will also be a general need for all colleagues within the organisation to have a basic level of knowledge of what the Council's approach is to managing its information and knowledge and what is expected of them as creators, users and providers/receivers of information and knowledge.

3.5 In terms of the specific skills and competencies that will be required to deliver the IKM agenda, a matrix has been produced (attached at appendix 1) which shows what is likely to be required to fulfil the range of roles and responsibilities that will be required.

3.6 The skills and competencies detailed in this matrix have been grouped around a number of key Information and Knowledge Management roles. However, it is expected that a wide range of roles may, over time, come to incorporate these sorts of skills and competencies. Such an example is the Stewardship role. These roles should play a vital role in ensuring that data, information and intelligence is managed and used appropriately and as an organisation we derive the best value from it. The concept of Stewardship and the associated roles and responsibilities is discussed in more detail at Section 4.0.

3.7 In reality, the Council could develop and put in place a range of strategies, policies and technologies to improve the way we store, manage, use and share our information and yet we may not realise the benefits of this effort. The difference will be seen if there is a shift in the culture within the organisation that sees information looked after and utilised as a strategic asset and there are individuals across the organisation who have responsibility and are accountable for the quality of data, information and intelligence. These roles are Stewardship roles - the trustees of our information assets.

4.0 STEWARDSHIP - WHAT IS IT AND WHY DO WE NEED IT?

4.1 Stewardship is the act of 'taking care of something'. Applied successfully it can ensure that there is a robustness to information quality that means that both data and information is an asset to the organisation.

4.2 Stewardship is most commonly applied to data quality and in this regard, Gartner state:

> *Most enterprises are realising that poor data quality is a significant inhibitor to the success of strategic business initiatives. Data quality issues make it difficult, if not impossible, to generate business value from customer relationship management (CRM), business intelligence (BI) or any effort requiring significant integration of data.*

4.3 This issue has been picked up by the Audit Commission who are keen – through CPA – to assess how the authority as a whole address data quality (and not just for statutory performance indicators); how this is managed, what strategies and policies are in place and how effectively these are put into practice across the whole organisation.

4.4 In 2006/07 the Audit Commission introduced Data Quality Key Lines of Enquiry (KLOEs) for the first time. Explicit and implicit within these KLOEs is the expectation that Local Authorities have assigned responsibilities at various levels of the organisation for data quality.

4.5 Given the above, it is clear that formal stewardship roles and responsibilities performed by individuals with appropriate skills and competencies will be an investment in our information assets. To take this forward within the Authority, it is proposed that an appropriate Stewardship framework is developed to support and embed the Skills and Competency Framework and is applied to both data quality and information quality. By developing such a framework, the Council will develop both data and Information stewardship arrangements to meet the KLOE requirements.

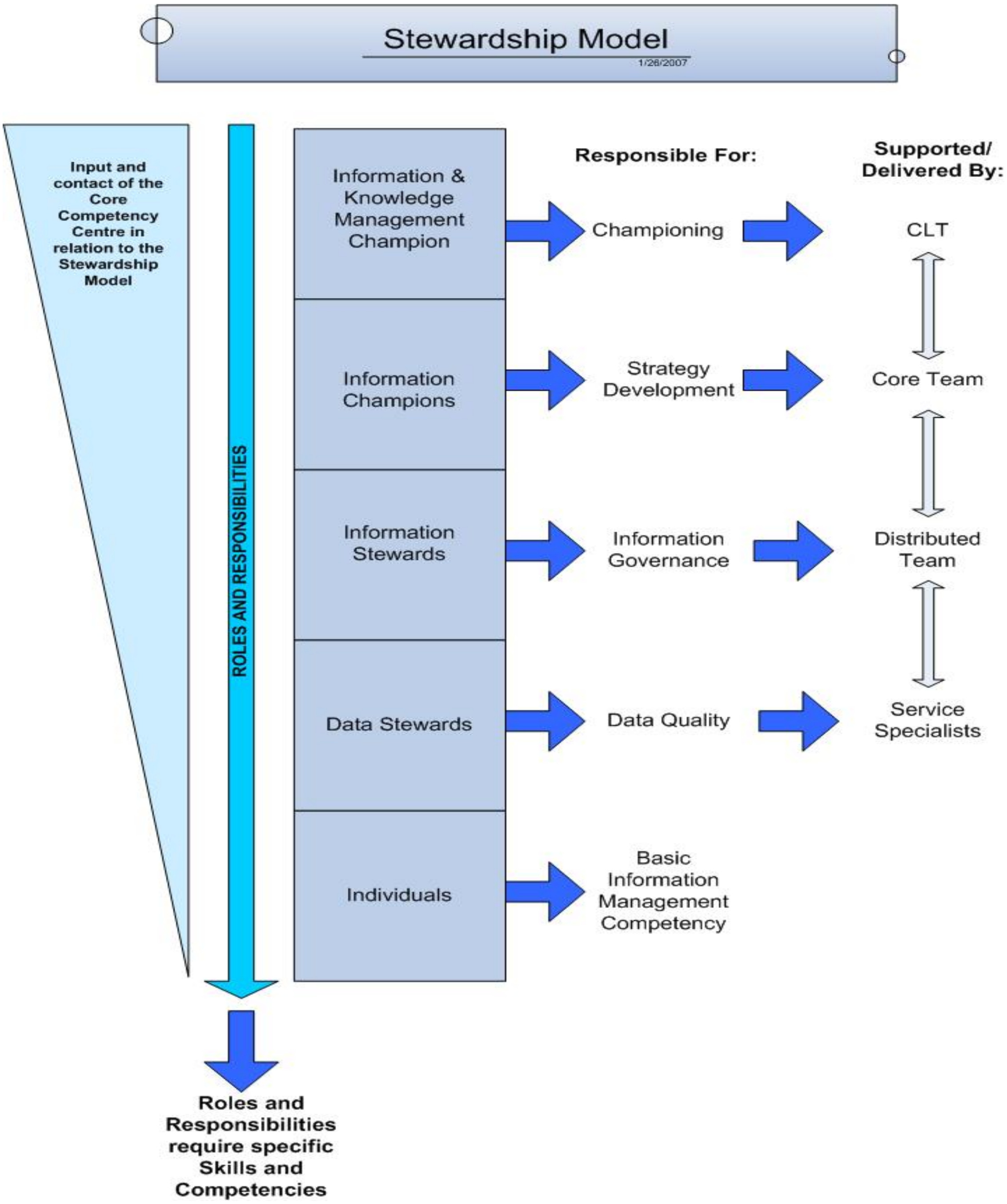
4.6 If such an approach were to be adopted within the authority, the likely roles and responsibilities of both information and data stewards would be as follows:

- To act as trustees (not owners) of manageable sets of information and data and ensure adequate quality is maintained to support the business.

- To work towards clear targets for information and data quality and be accountable for these.
- To facilitate the embedding of information and data quality in operational processes
- Be visible and respected within the organisation and seen as the leaders of information and data quality improvement efforts
- Where appropriate, undertake co-ordinated stewardship activity and develop stewardship policy at a strategic level.

5.0 STEWARDSHIP ROLES IN LEEDS

5.1 Taking the IKM Competency Centre model outlined above, it is envisaged that Stewardship responsibilities could operate as illustrated in the diagram below:


Stewardship Model
1/26/2007
Input and contact of the Core Competency Centre in relation to the Stewardship Model
ROLES AND RESPONSIBILITIES
Information & Knowledge Management Champion
Information Champions
Information Stewards
Data Stewards
Individuals
Responsible For:
Championing
Strategy Development
Information Governance
Data Quality
Basic Information Management Competency
Supported/ Delivered By:
CLT
Core Team
Distributed Team
Service Specialists
Roles and Responsibilities require specific Skills and Competencies

5.2 The diagram shows the various levels of stewardship responsibilities required as well as the roles envisaged for the different elements of the Competency Centre. Taking each in turn, their roles and competencies will be:

Information & Knowledge Management Champion

5.3 The Overall Information and Knowledge Champion will be the Assistant Chief Executive (Policy, Planning and Improvement). It is important that the agenda gets the highest profile and that there is a commitment to make things happen. By assigning responsibility at such a senior level it sends out the signal that the Council is serious about this agenda and can see the value in investing in it.

5.4 Listed below are a number of competencies that would be required from an Information and Knowledge Management Champion:

- Understanding of Information Governance including legislation, data sharing etc
- Understanding of the:
    - Document and Records Management;
    - Business Intelligence;
    - Collaboration agendas; and
    - the application and use of related technologies

5.5 These competencies would be complemented by specific skills and clear outlines or role and responsibilities.

Information Champions

5.6 The model shows that there would be Information Champions for the following major information and data types:

- person
- property
- staff
- finance

5.7 In terms of types of information, the majority of our data and information could be classified under one of these headings. Implicit within any discussion about these types of information is the fact that they cut across our organisational structure - whatever the structure. Trying to 'look after' and improve information across these areas will logically mean that there will need to be a greater level of co-operation and sharing of best practice across the organisation.

5.8 Managing our data, information and intelligence in this way will require high level championing and the commitment to ensuring that the best use is made of accurate and reliable data and information and that the organisation is able to benefit from the sharing of this information. In order to secure this high level championing these Information Champions should also sit on the Corporate Leadership Team (CLT).

5.9 The competencies required would reflect the competencies listed above for the Information and Knowledge Management Champion, whilst some of the specific skills, levels of skill and responsibilities required will be different.

Information Stewards

5.10 Information Stewards will be senior officers, typically heads of service. In the course of their existing role they will have responsibility for legacy systems such as the Academy system holding Benefits data. Information Stewards will be responsible for ensuring that data and information they look after is stored, made accessible, of good quality, shared, disposed of and used in compliance with any relevant standards or legislation.

5.11 Listed below are the competencies that would be required from an Information Steward:

- Understanding of Information Governance including legislation, data sharing etc
- Understanding Records Management principles and the application and use of related technologies

5.12 There would be a corresponding set of skills, skill levels and responsibilities under these competencies and these will be more detailed than those prescribed for the Information and Knowledge Management Champion and Information Champions.

Data Stewards

5.13 Data stewards will be responsible officers, with the appropriate skills, based in services who as part of their day to day role work closely with a particular data set (eg Benefits data). They will be responsible for improving the quality of data in their immediate area, managing access and permissions controls, ensuring data standards are adhered to and understanding the type, format and meaning of data held.

5.14 The competencies that would be required from a Data Steward are as follows:

- Understanding of Information Governance including legislation, data sharing etc
- Understanding of Data Management principles

5.15 The specific skills, levels of skill and competencies would be defined under these competencies.

Individuals

5.16 Individuals will, going forward will be made aware of their role and responsibilities in terms of Information Management. Individuals will be responsible for looking after data and information they create, use and share in accordance with the Council's policies. The introduction of a Core Information and Knowledge Management Competency is considered to be an important move to raise the profile of the importance of Information Management across the Council. Furthermore, the introduction of Information and Knowledge Management briefings as part of the new starter induction process as well as the incorporation of relevant Information and Knowledge Management related objectives within appraisals are also seen as important avenues for raising awareness and gaining commitment to how we manage and use our information assets.

5.17 Given the above, the development of a Stewardship function within the Council around the Information and Knowledge Management agenda to support the distributed Competency Centres will be instrumental in ensuring the information created, used and shared by the organisation is treated as a corporate asset of strategic value.

6.0 NEXT STEPS

6.1 The issues discussed above represent a change in culture for the Council and requires a different approach to how we perceive and value information. Overall it requires a commitment to appropriately organise resources to provide assurance that the information we use to make decisions is well managed, organised, robust, has integrity and is usable and accessible to those people who need it.

6.2 Given this, the following next steps will be taken:

- The concept of the distributed Competency Centre is developed in line with the One Council approach.
- Specific responsibilities within each 'part' of the Competency Centre will be clearly defined and allocated.
- A skills gap analysis is made comparing current capacity within the organisation to what is ideally required.
- A 'Chief Information and Knowledge Management Champion' is engaged and work is started with them to develop their role, responsibilities and competencies.
- Appropriate data stewards for all main legacy systems within the Council (e.g. Council Tax, Benefits etc.), are identified and work started with them on their roles, responsibilities and competencies
- Work is started with Corporate HR and Communications to identify ways to engage all colleagues in the IKM agenda to build their general understanding and also their responsibilities as employees of the Council in creating, managing, using and sharing information.

INFORMATION & KNOWLEDGE MANAGEMENT

IKM Skills and Competency Framework

Appendix 1

Draft S&C Matrix

Information and Knowledge Management

Skills and Competencies Matrix

Competency	Skill	Level of skill required					Core Comp	Dist Com Centre
		1	2	3	4	5		
Core Competency: Information and Knowledge Management								
Business Skills								
Strategic Policy Development	Link organisational objectives to strategic policy development							
	Role of best practice models into organisational context							
	Research skills							
	Strategy and Policy Development							
	Identification of resources to support I&KM initiatives							
	Identification of opportunities to develop I&KM initiatives							
	Information and Knowledge Management Agenda							
Business Change	Programme Management							
	Business Change Management							
	Translate business requirements into project deliverables							
Information Governance								
Information Governance	Operational Information Governance policies e.g. retention and disposition							
	Freedom of Information (FOI) legislation							
	Data Protection (DPA) legislation							
	Subject Access Requests							
	Information Governance frameworks to support I&KM initiatives							
Records Management	Records management principles							
	ISO 15489/ 0008							
	Retention and disposition policy and procedure							
	Classification schemes							
	Meta data standards							
	Effective search and retrieval methodologies							
	Technologies to support Document and Records Management (DRM)							
Data Management	Data quality issues							
	Data quality metrics							
	Data quality standards							
	Data profiling							
	Data integration issues							
	Information/ data sharing issues							
Business Intelligence								
Business Intelligence	Knowledge of the 5 styles of Business Intelligence (BI)							
	Knowledge of performance management principles							
	Knowledge of technologies to support BI							

Level 1 = Understanding of
Level 2 = Application of
Level 3 = Interpretation/Analysis of
Level 4 = Influence/Advise
Level 5 = Set policy/strategise

Competency	Skill	Level of skill required					Core Comp	Dist Com Centre
		1	2	3	4	5		
Core Competency: Information and Knowledge Management								
Content Management: Skills & Competencies to be identified as agenda progresses								
Collaboration and Learning: Skills & Competencies to be identified as agenda progresses								
Analytical Skills								
Data Interrogation	Exploration of data to discover patterns							
	Use of technology to exploit data							
	Data mining techniques; statistical analysis distribution and factor analysis							
	Spatial data analysis							
Data Interpretation	Distil relevant information and make recommendations							
	Cause and effect relationships							
	Data types across the organisation							
	Impact that the volume and reliability of data has							
Data Analysis	Build on-line analytical processing or multi-dimensional analysis							
	Techniques, ranging from simple data aggregation via statistical analysis to complex data mining							
	Advanced data analysis skills – evaluating statistical analysis distribution and factor analysis							
	Validation (during modelling and deployment) of analysis							
	Contextualisation of data analysis							
Process Improvement	Business Process Engineering							
	Business Process Management							
	Business Activity Monitoring							

Level 1 = Understanding of
Level 2 = Application of
Level 3 = Interpretation/Analysis of
Level 4 = Influence/Advise
Level 5 = Set policy/strategise

INFORMATION & KNOWLEDGE MANAGEMENT

Leeds CITY COUNCIL

Leeds City Council
Information Governance Framework

Appendix 1

The Information Governance Toolkit

Evidence-Based Scoring System for Assessing Information Governance Compliance

Level	Scoring Statement	Evidence	How?	Tools
0	There is no strategy or policies within the organisation. There is a lack of knowledge and understanding within the organisation and no awareness of the need to develop and establish a strategy and policies.	• There are no documented drivers or reports produced. No business case has been drafted.		TO BE DEVELOPED
1	There is an awareness and intent by the organisation of the need to develop a strategy, policies and procedures. Resources have been identified and responsibility assigned for this.	• The organisation has prepared an initial business case, drafted reports and developed documented drivers. • A communications plan has been prepared and all business requirements identified. • The organisation has determined audit outputs.	• Champions identified • Stakeholders identified • Research undertaken • Development plan prepared • The organisation has an understanding of the business need • Simple messages produced	TO BE DEVELOPED
2	A strategy, policies and procedures have been signed off and an implementation plan prepared. The organisation has assigned resources and has undertaken an information audit.	• The organisation has a documented strategy, policies and guidelines have been published and a communications plan publicised. • There is an implementation plan and training plan and capacity has been provided to carry this forward. • The organisation has put into place full monitoring and auditing procedures.	• Champions appointed • Information owners identified • Undertake approval process • Write policies • Develop plans • Commence communications exercise	TO BE DEVELOPED

Evidence-Based Scoring System for Assessing Information Governance Compliance (contd…)

3	An implementation programme is ongoing and has embedded policy and procedure in parts of the organisation. Improvement programme and governance arrangements are being applied across the organisation through systematic and continuous training.	• The organisation has an approved project management infrastructure to document the implementation programme. • Standards and procedures are in place and job descriptions and service improvement plans reflect this. • The organisation has agreed and published a full business case. • Appropriate resources have been trained and assigned responsibilities. • Training records are maintained. • Audit findings are published.	• An agreed full business case • Implementation plans • Training records • Roles & responsibilities (staff time) • Production of building blocks • Monitor & review • Resources secured	TO BE DEVELOPED
4	Policy and procedure is fully embedded and is integral to the organisation. Compliance and satisfaction are measured through effective monitoring and auditing procedures and the organisation is committed to maintaining and sustaining the programme.	• The organisation has project closure reports. • There is evidence of full compliance through Key Performance Indicators and regular audit reports. • The organisation has undertaken a full review against the business case and can ensure sustainability. • Outputs from the communication programme and satisfaction survey result have been published.	• Sustainable infrastructure • There are common systems throughout the organisation • Continuous communication • Continuous training • Monitoring & review • Audit process	TO BE DEVELOPED

INFORMATION & KNOWLEDGE MANAGEMENT

Leeds CITY COUNCIL

Leeds City Council
Information Governance Framework

Appendix 2

The Information Governance Workbook

INFORMATION & KNOWLEDGE MANAGEMENT

Leeds City Council

Information Governance Workbook

Contents

Step 1: Planning and Preparation

Purpose	
To ensure the work is properly planned, expected outcomes clearly defined and adequate resources committed	
Tasks	
Define the organisational scope	
Make the case for doing the work and secure management support	
Establish a project team and define their roles and responsibilities	
Ensure that project team members can provide the level of man-time required	
Agree arrangements for project supervision, monitoring and reporting of progress	
Develop an overall timetable for the project defining target dates for completion of each step	
Develop a high level project plan	
Make plans for briefing staff in the Business Unit about the project and their involvement in the work	

Step 2: Preliminary Investigation

Purpose	
Confirmation of exactly which parts of the council will be covered by this investigation (‘The Business Unit’)	
Confirmation of how the Business Unit is organised and relates to the rest of the council	
Development of a high level understanding of the work that the Business Unit carries out, the service it provides and who its ‘customers’ are	
Determining the legal and regulatory environment in which the Business Unit operates	
Identifying any specific drivers behind the Business Unit’s review of Information Governance needs	
Assessing the current state of the Information Governance arrangements (or infrastructure) in order to identify those areas where improvements are needed	
Outputs	
A document describing the organisational structure of the Business Unit	
A completed business profile questionnaire	
A completed Information Governance Infrastructure questionnaire	
An action plan setting out how gaps in the Information Governance Infrastructure will be closed	
Set of reference material collected during the course of the investigation	

Task 1: Profiling the Business Unit
3 man days to gather information and complete outputs
Some managers may need to be interviewed – 60 minutes per interview
Output 1 – Complete Business Unit Structure template
Captures a description of how the Business Unit is structured into different groups, sections and teams and how this relates to the overall structure of the council.
Information collected here will be used to identify the ownership and location of sets of information
The Structure is recorded in the form of a spreadsheet. Each column in the spreadsheet represents a different level in the organisation structure (the highest level being in the first column, the next level in the second and so on. Each row corresponds to a particular group or team in the structure
All levels of the Business Unit structure down to the smallest organisational unit should be covered
It is best to stick to existing structures which are well known, even if changes are due soon; the important thing is to be consistent throughout the exercise
Output 2 – Business Profile
Creates an overall picture of the Business Unit in terms of the work it does and the environment in which it operates
Only a high level overview is needed
The profile is captured using a questionnaire which is divided into the following sections: • **Background Information** – collects basic details about the Business Unit and identifies its main roles • Partners and Stakeholders – identifies the main groups with which the Business Unit interacts – this will help later with information sharing and security • **Regulation and Compliance** – identifies the legal and regulatory framework in which the Business Unit operates and how much this might impact the ways in which information is stored and used • **Business Drivers** – identifies business plans and objectives which might either impact this exercise or which are dependent upon its outcomes. It is clearly important to ensure that the results of this work are fully compatible with business needs

Task 2: Assessing Information Governance Infrastructure
2 man days to gather information and complete outputs
Some managers may need to be interviewed – 60 minutes per interview
Output 1 – Information Governance Infrastructure Assessment
Used to record and evaluate the current state of Information Governance in the Business Unit
Used to identify where there are deficiencies in current arrangements and to provide a framework for making improvements
Summary information is recorded using a questionnaire
The questionnaire is divided into the following sections: • **Organisation** – identifies where management responsibility for Information Governance lies, the level of resource committed to Information Governance and where policy is determined • **Policies and Procedures** – determines the currency, availability and coverage of Information Governance policy and procedure manual • **Awareness and Training** – examines how staff are made aware of Information Governance matters and the effectiveness of current training and communication arrangements
Output 2 – Information Governance Infrastructure Action Plan
Findings from the review should be reviewed and gaps identified
An action plan should be drawn up detailing what gaps need to be filled, what actions are needed, who will be responsible for carrying them out and when they need to be completed. It is not necessary to complete all of these actions before proceeding to the next stage of this workbook although most policies and procedures will need to be in place before Step 5 can be completed

- **Organisational Gaps** – guidance on roles and responsibilities and reporting structures is provided. The chosen structures and roles and responsibilities should be embodied in an Information Governance policy statement
- **Policy and Procedure Gaps** – It will be necessary to determine who will be responsible for development and ongoing maintenance of policy and procedure statements. Where policies and procedures already exist it is recommended that these should be reviewed if this has not been done recently. Where none are available then it may be possible to draw upon corporately available material
- **Awareness and Training Gaps** – training material and assistance may be available corporately

Step 3: Determining Information Governance Needs

Purpose
Development of a complete picture of all the activities carried out by the Business Unit and how they interrelate
A summary of what principal sets of records need to be generated from these activities and how they should be managed
Outputs
A Functions and Activities Model describing all of the functions performed by the Business Unit and the individual activities carried out in fulfilling those functions
A description of the record keeping requirement for each activity
Further reference material collected during the course of the investigation
Task 1: Functions and Activities Analysis
5 man days to gather the information required and complete the outputs
Some managers, supervisors or administrators may need to be interviewed. Interviews should be no more than 60 minutes each
Output 1 – Functions and Activities Model
This will create a high level model of the work carried out by the Business Unit
It is a list of business functions broken down into activities which are in turn broken down into sub-activities
• Functions correspond to the primary purposes or goals of the Business Unit • Activities correspond to the way in which work is broadly divided up in order to fulfil these goals • Sub-activities correspond to the individual streams of work which make up each of these activities

For each group identified in Task 1, Output 1 (Business Unit Structure), a summary of the services provided and the individual activities carried out in delivering those services should be developed. This may be drawn from published sources, internal documents or through interview

Having developed a list for all groups then each entry in the summary should be matched to an entry (or entries) in the council's standard Function and Activity Classification List. It may be necessary to either group or split summary entries to obtain a match. There may be exceptional circumstances where there isn't a good match in which case additions to the Classification List can be made

The results of this analysis should be recorded in Figure E. Columns in the spreadsheet correspond to Functions, Activities and Sub-Activities. Each row corresponds to a particular sub-activity

Task 2: Record Keeping Requirements Analysis

4 man days to gather the information required and complete the outputs

Some managers, supervisors or administrators may need to be interviewed. Interviews should be no more than 60 minutes each

Output 1 – Record Keeping Requirements Analysis

Used to document identified record keeping requirements for each of the areas of activity identified in the previous task

Provides an opportunity to clarify real record keeping requirements in the Business Unit; there may be instances where records currently are either being kept unnecessarily or are not being held in accordance with specified rules

Requirements should be identified by investigating the following:

- Legal and regulatory constraints
- Obligations placed on the council by stakeholders
- Best practice standards recommended by professional bodies
- Council policies
- Departmental procedures

Exhaustive coverage of every possible requirement is not essential. The recommendation is to focus on the most significant record keeping needs which would include:

- Records which are critical to operation of the Business Unit
- Sets of records which are likely to be substantial in size
- Those records which are subject to strong external regulation in terms of their creation and use

A spreadsheet is provided for capturing findings; a separate questionnaire worksheet is used to document the Record Keeping needs for each Activity/Sub-Activity. The questionnaire is divided into the following sections:

- Identified Record Keeping Requirement – outlines the scope and content of a set of records that need to be kept (a separate column is used for each distinct set of records)
- Reasons – identifies why the records need to be kept and identifies the source of any policies, agreements or legislation that determine this need
- Access Needs – documents who needs to be able to access all or some content of the records
- Specific Needs – identifies any known Information Governance needs such as retention periods, storage formats and security measures

Step 4: Information and Records Management Survey

Purpose

To identify all of the sets of documents or records collections held by the Business Unit together with details of their current storage and management arrangements

Outputs

A set of completed survey questionnaires

A Records Inventory spreadsheet cataloguing all sets of records held by the Business Unit

Task 1: Preparing for the Survey

10 man days to complete all necessary activities

Output 1 – Planning the Survey

Information is collected through completion of a separate questionnaire for each ‘Record Collection’ in the Business Unit and through direct inspection/investigation where required. A decision needs to be taken on the best way of organising this work; one of two basic strategies for carrying out the survey can be chosen:

- Devolved or Managed Survey – identified contacts in different parts of the Business Unit are tasked with ensuring that questionnaires are completed for their part of the organisation. Returns are collated and vetted centrally within the Business Unit. Follow up interviews are carried out in order to clarify information in the survey returns and to fill gaps. This approach is likely to be the quickest for larger Business Units but has a greater administrative burden. This approach requires that contacts are well briefed and it is highly likely that follow up investigations will be required.
- Centralised Survey – all of the survey work is carried out centrally in the Business Unit (i.e. one person/group visits all areas and carries out investigations/interviews and completes questionnaires directly) Contacts across the Business Unit still need to be identified but their role is one of facilitating the survey rather than ensuring that questionnaires are completed. This approach is likely to be the most accurate but may be time consuming/impractical for larger Business Units

A network of contacts needs to be identified. All parts of the organisation must be covered by the contacts

People with some or all of the following attributes would make a good choice for contacts:

- Familiar with the sets of filing in use (e.g. administrative/support staff)
- Have specific responsibility for the day to day management of information in the Business Unit
- Known custodians of major sets of information
- Experienced staff with good familiarity with the work of the Business Unit
- Have sufficient respect/authority to be able to secure the cooperation of other staff in the Business Unit

The following administrative arrangements should be addressed as a minimum:

- Methods used for issuing and collecting questionnaires. In order to simplify the capture, collation and analysis of returns questionnaires should be completed electronically. It needs to be decided if these will be distributed by email or if a common shared folder will be used.
- File-naming conventions. It is strongly recommended that a standard system for naming completed questionnaire files is defined. This is needed to ensure that all returns are uniquely identified and can be easily related to the part of the organisation from where they came
- Progress management. Arrangements need to be in place to monitor the return of questionnaires in order to ensure that all parts of the Business Unit are covered, that returns are completed on time and that missing material can be chased.

Output 2 – Survey Questionnaire Design

A questionnaire template is provided and major changes are not advised. However, the following changes may be needed:

- Adding the ‘who to contact for help’ section in the notes and instructions panel
- Pre-populating the Completion Details section with department/group/team names
- Changing the terminology and examples given to mirror those used in the Business Unit
- Adding further questions of specific interest to the Business Unit
- Creating a ‘light’ version of the questionnaire containing a subset of questions to be answered by recipients (with the other questions being answered in follow-up investigations)

The purpose of each section of the questionnaire is as follows:

Section 1 – Completion Details

Largely self explanatory, this section collects names and contact details of the person completing the questionnaire (not necessarily the same as the ‘owner’ of the record collection described) Ideally the organisational levels should coincide with those identified in the Business Unit Structure

Section 2 – Record Collection Description
Collects basic descriptive information about the Record Collection concerned. The answers to questions 2.4 and 2.5 will be used later to assist in linking the collection to the Functions and Activities model. Question 2.6 helps to determine if the records may be covered by DPA rules and it may be appropriate to index files using personal IDs of some form. Question 2.7 helps to identify if the records could be indexed using standard Unique Property Reference Numbers (UPRN). Question 2.8 helps to identify if records could be linked to Geographic Information Systems (GIS) if required

Section 3 – Record Collection Organisation
Identifies the ways in which the collection is structured and identified. Answers to Questions 3.4 to 3.7 will be used to help define a common indexing scheme (or 'metadata' scheme) which would be used in an EDRMS. Question 3.8 identifies if all or some of the records are duplicates of other information held elsewhere

Section 4 – Storage Details (Paper)
Where material is held on paper this section gathers information about current storage arrangements. The section collects information about storage space needs which could be used for storage planning purposes and to assist in making business cases for migrating to electronic storage. The section also examines the security and protection arrangements for the records to determine if improvements may be needed

Section 5 – Storage Details (Electronic)
This section collects information about electronic storage arrangements where appropriate. This again looks at storage space requirements which may assist in future IT planning. The section is also used to assess whether improvements may need to be made to security and backup arrangements

Section 6 – Access and Retention
This section examines current access arrangements for the records (who can access them and how access is provided). The section also investigates how retention management policies operate. The information describing actual practice gathered here will be compared with the requirements identified in the Record Keeping Needs Analysis

Output 3 – Briefing Material

A briefing session should be held to ensure that all contacts are fully conversant with the aims of the survey and fully understand the process that will be followed

The following topics should be covered:

- Survey aims and objectives – these should cover both council corporate objectives and the specific reasons why the Business Unit is carrying out the work
- A description of the overall survey process and the steps that will be followed
- Detailed description of how to complete the questionnaire, including a live demonstration of using the spreadsheet file
- Details of the administrative arrangements and the required timetable

Task 2: Conducting the Survey
3 weeks between distribution and return of questionnaires
Output 1 – Register of Survey Returns
Issuing of questionnaires should coincide with the completion of briefing sessions in Task 1, Output 3
A deadline should be set for completion and returns should be actively chased and reminders issued near to the closing date
A register of returns should be kept as returns are received to make it easier to spot gaps in coverage and to make it easier to avoid duplication of returns
The returned spreadsheet files should be retained and kept well organised for future reference
Individual questionnaires should be reviewed to look for areas where: • Important answers have not been provided or where recipients have obviously struggled to provide the information required • Information provided is clearly incorrect or confusing • Issues have been raised that are worth further investigation
The overall set of returns should also be assessed to: • Look for obvious gaps in coverage (e.g. areas where one might expect records to exist and none have been reported). It is advisable to review the Record Keeping Needs Analysis to check if all sets of required records have been identified in the survey • Ensure that all functions/activities identified have been covered • Look for contradictions in the information provided or for duplication (e.g. more than one person has reported what appears to be the same collection)
A list of areas warranting further investigation can be drawn up from the above validation exercise and follow up interviews/phone calls should be carried out as required
100% accuracy should not be expected and so follow up work should focus on what are deemed to be the most important areas
Task 3: Building the Inventory
5 man days to complete

Output 1 – Records Inventory
A template is provided for the inventory to a corporate standard so major change should not be made. The following changes may be needed: • Adjusting the columns in the inventory to match the questions asked in the inventory • Alterations to the way in which the inventory can be displayed on screen and printed
The answers to all the questionnaires need to be loaded in to the inventory. Raw data can be copied and pasted from each of the returned questionnaires
All entries need to be checked and adjusted; this can either be done as each questionnaire is loaded or after all of the raw data has been loaded.
The following adjustments may be needed: • 'Normalisation' of column entries to make them all consistent. This aids subsequent searching and analysis e.g. ensuring that department/team/group names are consistent makes it easy to then identify all entries for a particular group in the council • Ensuring that numeric values have been entered as numbers and that units of measure are consistent where this is important to analysis e.g. ensuring that all file storage volumes are stated in linear metres would make it easy to quickly calculate total storage volumes • Identifying collections which have been reported more than once and ensuring that they are entered only once in the inventory

Step 5: Classification

Purpose
Definition of a 'Records Classification Scheme' which can be used to help organise all the sets of records identified in step 3
Organising the Business Unit's information under this scheme
Making linkage of the classification scheme to ownership, retention, security, access and sharing rules thereby ensuring that all sets of information can be correctly managed
Planning for development of the above to provide a complete 'fileplan' (including identification of how records will be indexed and identified in order to support their retrieval)
Outputs
Classification Scheme Design for the Business Unit
All records held by the Business Unit classified under this scheme and linked to Information Governance rules
An outline implementation plan for changes needed to current practice
Task 1: Designing the Classification Scheme
3 man days to complete
Output 1 – Classification Scheme Design
Attempt to place each of the collections in the inventory into the classification scheme using the classification spreadsheet. Each collection should only fall into one classification but a single classification can cover more than one collection. Do not modify the classification scheme at this stage but note which collections don't fit
For those collections that do not appear to have an appropriate classification entry at all, new classifications should now be added
If a collection appears to fall into more than one classification then it may actually be more than one collection that has been misreported as a single collection during the survey in which case it may be appropriate to split it up and classify different parts separately

Alternatively it may need to be treated as a case file or other non-functional element – this is likely to be the case if the collection maps to a single level 2 classification but not at lower levels. Careful consideration needs to be given to the nature of the collection before treating the collection in this manner and adjusting the classification scheme to accommodate it
Consideration should also be given to whether problems of classifying collections are caused by inappropriate definition or choice of classifications in the outline scheme in which case adjustments should be made
Lower levels should now be added to the scheme as required. This will be needed where the classification scheme is 'crowded' (many collections under the same classification) or where several obviously very different collections fall into the same classification
This process may also highlight collections reported in the survey which should be merged and treated as a single collection
The process above should be continued until all collections have been classified
After changes have been made to the classification scheme it is advisable to check to see if the original classification decisions made in the first stage are still the most appropriate. This could be checked by repeating the exercise of classifying all of the collections against the adjusted scheme
It is suggested that occasional 'snapshots' of working versions of the scheme are saved as it evolves to enable back-tracking if it is required
Task 2: Expanding the Classification Scheme
5 man days to complete
Output 2 – Expanded Classification Scheme
Use the classification scheme spreadsheet to process each entry in the classification scheme and to determine the governance that should apply to that entry
Select the classification entry and review the contents of the Record Keeping Needs Analysis to identify what requirements were documented for records associated with the relevant functions and activities
Review the contents of the Records Inventory to locate the entries corresponding to the record collections placed under this classification
Using the two sets of information above and making reference to relevant policies and procedures work through each of the categories of Information Governance rules described below and decide what rules should apply. In some cases further investigation or analysis may be required to make decisions

Information governance rules should be similar for all folders within a specific classification. If this is not the case then adjustments may need to be made to the classification scheme (such as adding a further level of classification) keep track of changes using version control columns in the spreadsheet
Before moving on to the next classification entry make a note of any gaps between the decisions made and current practice to provide the basis of an implementation action plan
Information Governance areas to be included are:
Ownership
This should be the title of an organisational unit rather than named individuals
Staff within the owner unit will be given specific responsibilities e.g. reviewing, disposal, ensuring quality etc
Storage
Decisions should be taken on the appropriate storage medium e.g. paper, electronic, microfilm and where these will be stored
These should be looked at for the 3 stages in the record lifecycle – current, semi-current, archive
Legislative requirements, access needs, security needs and legal admissibility all need to be accounted for when considering storage
Special storage or protection measures may need to be considered if the records are vital
Procedures must also be defined for when records are migrated between formats and/or storage locations
Access and Sharing
By default records should be marked as Unclassified and should be accessible by any council employee, reasons for restricting access should be noted (e.g. contain personal information, commercially sensitive etc.) Decisions will be influenced by security policy and legislative constraints
Any requirements to be able to share material with partners or other third parties also need to be recorded. Reference should be made to any supporting agreements or protocols that apply
Disclosability under FOI, DPA and EIR legislation should also be decided. Reasons for exemptions should be recorded

Access rules can be recorded by:

- Assigning a security category or ‘marking’ to the classification (e.g. Restricted, Highly Confidential, Confidential and Unclassified) these categories are generally defined corporately and define basic access rights (e.g. only the most senior staff would have access to material marked Restricted); or
- Linking access groups or named individuals to classifications. Access groups may correspond to organisational units (e.g. only staff in a ‘personnel’ group can access employee files). Security markings and access groups can overlap (e.g. only senior managers with rights to see Highly Confidential material in Personnel can access Disciplinary and Grievance records in employee files)

Retention and Disposal

Rules should be able to be determined using the corporate retention schedule

Retention rules can be recorded in the following way:

- A ‘disposal action’ (e.g. Destroy, Retain for Further Review, Transfer) – allowable actions will be set out in policy documents. Policies will also define how actions should be carried out (e.g. whether secure destruction is needed)
- A ‘Period’ – the period of time after which the action should be invoked
- An ‘Event’ (if appropriate) – an event which determines when the ‘Period’ begins

An example of this would be:

- Disposal action = Destroy
- Period = 7 years after the event
- Event = End of employment

A link to the relevant to retention schedule entry should be maintained as this will make it easier to change rules if retention policy changes

Creation

Any specific policies and procedures that should apply to the ways in which records are created and modified need to be identified and recorded. Examples include:

- Document scanning procedures – may be of particular importance when ensuring legal admissibility of stored images is a significant requirement
- Data quality standards or methods which should be applied – it may be important to be able to evidence that these have been followed in order to assess the accuracy of information held
- Procedures governing approval and issue of documents – this may be needed where it is important to record evidence of approval of key documents such as policy statements or where it is necessary to record evidence of when documents were issued/published
- The need to keep audit trails to demonstrate the provenance or identify the revision history of material – may be important in areas subject to regular audit or external scrutiny

Indexing/Metadata Needs

Indexing terms or metadata needs should be determined; these will be needed for EDRMS implementation. In an EDRMS metadata can be attached at both folder and individual record levels.

A corporate metadata standard defines what metadata terms must be applied to all of the Council's records.

The corporate metadata standard should be reviewed and the following decisions made:

- The standard will identify some terms as being mandatory but others will be optional; it needs to be determined whether any of the optional terms should be made mandatory within the Business Unit or for certain classes of records
- Lists of allowable values may be defined for some terms, these lists should be reviewed for suitability. The need for any additional values would need to be raised with those responsible for corporate standards. It may also be possible to define a subset of these values (or even a single value) which should apply to the record class

It is advisable to minimise the number of metadata terms and to utilise corporate standard metadata terms wherever possible but it may be necessary to also identify additional 'user-defined' terms to meet local needs. The number of user-defined terms allowed may depend upon the choice of EDRMS.

Circumstances where additional metadata may be required include:

- Where records are organised or indexed in a particular way to suit operational needs (e.g. by Supplier Name or by Purchase Order)
- Where it is necessary to be able to link records or folders to business systems by means of a unique system reference (e.g. employee number)
- Where it is necessary to be able to link material to a GIS system by means of a location or property identifier

If user-defined metadata terms are needed then these should be documented with consideration being given to:

- How practical it will be for users to supply this metadata when registering new items
- Whether they should adhere to specified formats (e.g. date format, numeric etc)
- Whether allowable values should be defined in 'controlled lists' and if so how they would be generated (e.g. from a database) and how they will be maintained

Output 3 – Outline Implementation Plan

In the course of completing this step a lot of decisions will have been made that will need to be put into action. An action plan should be drawn up detailing what changes may be needed, what actions are required to put them into place, who will be responsible for carrying them out and when they need to be completed.

Actions will fall into different categories

Working Practice Changes

- Decisions made may require changes to the ways in which staff carry out some of their work (e.g. by filing material in a different way, adopting new file-naming conventions for electronic files etc)
- Current departmental procedures may need to be updated and staff made aware of how practices need to change

Reorganisation of information

Some decisions may require actions to ways in which current information is held, examples may include:

- Reorganising shared server folders
- Moving paper filing offsite or other storage locations
- ‘Weeding’ existing collections to dispose of unwanted material so that it can be managed/stored more easily

EDRM Dependent Actions

Some decisions will require actions that need to be built into EDRM implementation plans, these will include:

- Detailing decisions on fileplan design including metadata definitions and folder requirements
- Organising the back-scanning of paper filing to be migrated into the EDRMS
- Detailing how access control lists should be defined

Skills and Competencies

Some changes may require that some staff be given greater responsibility for Information Governance matters. It will be necessary to ensure that all staff understand what their responsibilities are and have been given the necessary training and guidance to fulfil them.

Step 6: Policies and Procedures

Purpose
Raise the level of Information Governance to meet the unit’s requirements for compliance and efficiency
Ensure that any technology implemented meets the appropriate compliance and efficiency requirements
Outputs
Complete set of all policies and procedures required for the management of information in the unit
A matrix of the current status of corporate policy and procedure documents and business unit policy and procedure documents
Task 1: Developing Policies and Procedures
Policies should be short documents, outlining high-level requirements and roles and responsibilities but without specific details that would get out of date quickly
Policies should be signed off by the appropriate board or member of senior management
Each policy document should include the following headings: • Overview • Scope • Compliance • Responsibilities • Consultation • Policy statements
Procedures should be as long and detailed as they need to be to cover the material, but should be user-friendly documents suited to the audience. They should include the following headings: • Overview • Scope • Responsibilities • Procedures

All policies and procedures should be numbered, version controlled and cross-referenced
Policy documents should be signed off at a high level by the appropriate board member or member of senior management
Documents should have a document control table with a history of versions and changes and the next review date, which will be around 2 years for a procedure document and around 5 years for a policy document
Output 1 – Corporate information governance policy and procedures
This output is focussed on corporate policies and procedures
Start with the policies identified in the Information Governance Infrastructure Assessment and check them for accuracy and currency
Create a gap analysis between the existing documents created in the Information Governance Infrastructure and the list of documents in the Record Keeping Requirements Analysis
The missing documents must be written, finalised and approved
Necessary policies and procedures are:
Information Management Policy • Definition of records and information • Policy statement on corporate ownership/local custodianship • Principles of information management • Policy statement(s) for each of the topics listed below
Internet Guidance • Acceptable use • Downloads • Monitoring

Email Guidance

- Email message contents and headings
- Protocols for replying and forwarding
- Use of attachments
- Storage
- Personal emails
- Distribution lists
- Spam and chain emails
- Viruses
- Out-of-office messages
- Archiving
- Monitoring

Your information, your responsibility – Handbook for Leeds City Council employees and contractors

- IM principles
- Record keeping duties
- Use of personal and shared drives
- Use of mobile devices (memory sticks, CDs, laptops, PDAs)
- Templates
- Naming conventions
- Version control
- Duplication
- Monitoring
- Scanning
- Printing

Information Sharing Protocol (to be followed by a set of ISAs for each Business Unit)

- Parties to the protocol
- Purposes of information sharing
- Principles of information sharing
- Procedures
- Monitoring

FOI, EIR and DPA Access Requests

- Identification of information access requests
- Timing and fees
- Release decisions
- Responding
- Complaints and appeals
- Monitoring

Data Quality

- Purposes: compliance, decision making, risk-reduction
- Principles: accuracy, completeness, relevance, timeliness, availability
- Referencing standards: GDSC (Government Data Standards Catalogue)
- Methods: data entry validation, system integration, de-duplication, training
- External contracts: building in quality
- Monitoring

Access and Permission Controls

- Principles of openness and confidentiality
- Roles and rights
- Joined up working
- Monitoring

Security Policy

- Principles of: availability, authenticity, confidentiality, integrity, non-repudiation
- Physical and IT security
- Clear-desk policy
- Monitoring

Storage and Handling Guidance

- Physical storage
- Off-site storage
- Equipment
- Handling guidance
- Monitoring

Retention and Disposal

- Retention principles
- Disposal methods
- Retention schedules
- Monitoring

Preservation and Future-Proofing

- Lifecycle management of records
- Suitable media and formats
- Preservation methods: technology watch and document conversion
- Quality assurance of IT projects for: record-keeping implications, document tracking, exit strategies
- Emerging technologies
- Monitoring

Accountability and Legal Admissibility

- Storage options
- Information capture procedures
- System maintenance
- Audit trails
- Document tracking
- Discovery methods
- Authenticated output
- Monitoring

Business Continuity Planning

- Risk assessments
- Overall plan
- Testing
- Monitoring

Output 2 – Business Unit information governance policy and procedures

Start with the local policies identified in the Information Governance Infrastructure Assessment and check them for accuracy and currency

Create a gap analysis between the existing documents created in the Information Governance Infrastructure and the list of documents in the Record Keeping Requirements Analysis
The missing documents must be written, finalised and approved
The policy and procedure documents required at business unit level may include:
Information Sharing Agreements • Reference to the Information Sharing Protocol • Parties to the agreement • Purposes of information sharing • Information to be shared • Roles and responsibilities
Scanning Procedures – reference to Accountability and Legal Admissibility • Sorting and preparing paper for scanning • Quality assurance • Checking paper scanner performance • Rescanning • Indexing • Retention and disposal of originals