Central Bedfordshire Council

Information and Records Management Policy

Version 0.5

March 2009

Not Protected

Policy Governance

Accountable Director	
Policy Author (Title)	
Approved By (Title)	
Date Approved	
Issue Date	
Review Date	
Person Responsible for Review (Title)	
Include in Publication Scheme (Y/N)	
Publish to Web (Y/N)	
Intranet Link	
Circulation	This policy is to be made available to all CBC staff and observed by all members of staff, both social care and otherwise. There will be an ongoing professional development and educational strategy to accompany the implementation of this policy.
Implementation Plan in place (Y/N)	

Policy Approval

Central Bedfordshire Council (CBC) acknowledges that information is a valuable asset. It is therefore wholly in its interest to ensure that the information it holds, in whatever form, is appropriately governed, in terms of protecting the interests of all of its stakeholders.

This policy and its supporting standards and work instructions are fully endorsed by the Council Executive through the production of these documents and their minuted approval.

I trust that all staff, contractors and other relevant parties will, therefore, ensure that these are observed in order that we may contribute to the achievement of the Council's objectives and the delivery of effective services to our community.

Chief Executive: ______________________________

Date ______________________________

The current version of the Central Bedfordshire Council's Information & Records Management Policy is available from the website at www.centralbedfordshire.gov.uk.

Alternatively, a copy can be obtained by writing to the Information Governance Manager at:

Central Beds Council
Priory House
Chicksands
Shefford
SG17 5TQ

Revision history

Version Number	Revision Date	Summary of Changes	Author
0.1	05 Feb 2009	Draft	Rob Hutton
0.2	14 Feb 2009	Revision	Rob Hutton
0.3	19 Feb 2009	Revision	Rob Hutton
0.4	23 Feb 2009	Revision	Rob Hutton
0.5	4 Mar 2009	Revision	Rob Wood

Contents

Glossary

Access	The right, opportunity, means of finding, using or retrieving information. [ISO 15489]
Accountability	The principle that individuals, organisations, and the community are responsible for their actions and may be required to explain them to others. [ISO 15489]
Classification	Systematic identification and arrangement of business activities and/or records into categories according to logically structured conventions, methods, and procedural rules represented in a classification system. [ISO 15489] See also Security Classification
Conversion	Process of changing records from one medium to another or from one format to another. [ISO 15489]
Core Records	Records, in whatever form, that are required for permanent retention
The Council	For the purposes of this document this refers to Central Bedfordshire Council.
Destruction	Process of eliminating or deleting records, beyond any possible reconstruction. [ISO 15489]
Disposition (keeping, moving or removing records)	Range of processes associated with deciding whether to keep, destroy, or transfer records. These are documented in disposition authorities, retention schedules or other instruments. [ISO 15489]
Document (noun)	Recorded information or object which can be treated as a unit. [ISO 15489]
EDRM	Electronic Document and Records Management – the process of managing records (both physical and electronic) in an electronic environment
EDRMS	Electronic Document and Records Management System – the software and hardware used to manage records in an electronic environment.
Indexing	Process of creating access points to facilitate retrieval of records and/or Information. [ISO 15489]
Metadata	Data describing context, content and structure of records and their management through time. [ISO 15489]
Migration	Process of moving records from one system to another, while maintaining The records' authenticity, integrity, reliability and usability. [ISO 15489]
Preservation	Processes and operations involved in ensuring the technical and intellectual survival of authentic records through time. [ISO 15489]
Records	Information created, received and maintained as evidence by an organisation or person, in pursuance of legal obligations or in the transaction of business. [ISO 15489]
Record lifecycle	Term used to describe the life of a record in the organisation from origination through to its disposal.
Records management	Field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, retrieval, use and disposition of records. These include processes for capturing and maintaining evidence of, and information about, business activities and transactions in the form of records.[Based on ISO 15489]
Record series	A group of related records that are normally used and filed together or otherwise linked, and that allow consideration as a unit for use, review,

	retention or destruction purposes.
Registration	Act of giving a record a unique identifier on its entry into a system. [ISO 15489]
Retention schedule	Schedule that outlines the specific time periods for the retention of records (see also disposition)
Security Classification	Defines the handling, storage and disposal arrangements required to protect the material to a level appropriate to its sensitivity.
Tracking	Creating, capturing and maintaining information about the movement and use of records. [ISO 15489]
Vital records	Records, in whatever form, that are essential to the continued operation of the Council after a disaster (business recovery).

1. Introduction

Having accurate, relevant and accessible information is vital to the efficient management of the Council, which values records and information as important corporate assets. The Council must balance its statutory obligations in this area (for example providing the public with access to information) with its aim to be open and responsive, and with its duties of confidentiality for personal and commercially sensitive records and information. This balance requires the Council to create and manage all records efficiently, make them accessible when needed, protect and store them securely and dispose of them safely at the appropriate time.

The Council complies with all relevant legislation and aims to achieve high standards of best practice. This includes the adoption of principles from recognised bodies such as the British Standards Institute (BSI) and the International Organisation for Standardisation (ISO).

The Council makes sure that:

- Officers have access to records management training
- Officers are encouraged to manage records and information properly
- Supporting standards, procedures and guidelines are provided
- Compliance is monitored via a clear process
- This policy is reviewed regularly to ensure that is remains relevant.

This policy is designed to be the cornerstone of corporate information and records management. Any directorate protocols and procedures in this area must be consistent with this policy. Should a conflict arise then the corporate policy takes precedence.

2. Scope

The purpose of this document is to define the elements of the Council's Information and records management policy, which include:

- Defining the meaning and concepts of information and records management
- The management of paper records
- The management of electronic records
- The management of archival records
- Information and records security
- Roles and responsibilities of officers and users of the Council's information and records
- The policy's relationship with other legislation and policies

2.1 Information and Records Management

Good information and records management relies on the following principles being applied:

- The regular review of information and record holdings
- The controlled retention of information
- The controlled disposal of information

Good management of records, and information contained within them, benefits the Council through:

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

The guiding principle of information and records management is to ensure that information and records are managed through their full life-cycle, from origination of a record, maintenance, managing its use, access to it, storage, retrieval and finally disposal of the record.

The Council is required by law to manage its records properly. Statutes such as the Local Government Act 1972, the Data Protection Act 1998 (DPA) and the Freedom of Information Act 2000 (FOIA) are particularly relevant, as they set out specific requirements for the creation and management of information and records.

A list of other relevant legislation and standards can be found in Appendix C

This policy aims to make sure that all Council officers, and other users of the Council's records and information, understand what they must do to protect and manage records and information effectively, efficiently and economically.

This policy is supported by a set of information records management guidelines, which the Council as a whole must follow.

The policy is based on the international standard for records management ISO15489.

Each Directorate is responsible for ensuring that its day-to-day working procedures and practices incorporate the corporate records and information requirements.

2.2 What does this policy apply to?

This policy and the guidelines that support it apply to the management of information and records, in all technical or physical formats or media, created or received by the Council while carrying out its business activities.

Although this is not an exhaustive list, examples of items that can be records include:

- documents (including written and typed documents and annotated copies);
- paper-based files;
- electronic files (including word processed documents, databases, spreadsheets and presentations);
- electronic mail messages (email);
- diaries;
- faxes;
- brochures and reports;
- intranet and internet web pages;
- forms;
- seized evidence;
- audio and video tapes, including CCTV
- microfiche and microfilm;
- maps and plans; and
- photographs

2.3 Whom does this policy apply to?

This policy and the guidelines that support it apply to all permanent and temporary employees, contractors, consultants and secondees who have access to Council records and information, wherever these records are located and whatever form they are in.

2.4 Why do we need to manage records?

Maintaining efficient records management practices helps us meet our statutory objectives and overall business responsibilities as an effective local authority. Whatever form the record takes, knowledge and information must be protected. It must also be accurate, ordered, complete, useful, up-to-date and accessible whenever it is needed to:

- deliver effective public services and carry out our business;
- comply with relevant legislation
- support research and development;
- help us all make informed decisions;
- keep track of policy changes;
- ensure that legal precedents are identified;
- support continuity and consistency in management and administration;
- protect the rights of employees, regulated entities and the general public;
- provide an audit trail to meet business, regulatory and legal requirements;
- make sure that we work effectively as a regulator and prosecuting authority and meet our lawful obligations for disclosing evidence;

- promote our activities and achievements; and
- make sure we are open and responsive, as set out in our Vision and Values and as required under FOIA

3. Roles and responsibilities

3.1 Central Bedfordshire Council

The Council owns all records and information created by officers[1] carrying out Council business-related activities, unless the originator keeps ownership (such as intellectual property information and/or records outlined in a contract with a third party).

Records received by Council Officers are also the responsibility of the Council. Individual employees do not own records but they do have responsibilities for managing records.

3.2 Executive responsibility

Members of the Executive have overall executive responsibility for Council records and information management policy and guidelines, and supporting their application throughout the organisation.

Individual Directors have responsibility for ensuring that local procedures are in place and that records management, including review, file tracking and destruction, is carried out in accordance with those procedures.

3.3 Information and Records Management team responsibilities

The Information and Records Management team (IRM), has the following responsibilities:

- Policy and standards - making sure that the records management policy and guidelines are kept up-to-date and relevant to the needs and obligations of the organisation.

- Communication and awareness - ensuring training and information mechanisms are in place for instructing officers in their roles and responsibilities in relation to the information and records management function and for ensuring that all staff are aware of the corporate policies and guidelines for information and records management

- Advice and guidance - providing information and records management advice and guidance to line managers, or their delegated ‘records management’ staff.

- Monitoring – monitoring the information and records management practices of the organisation and ensuring that they meet the requirements laid out in this policy and any related procedures.

[1] In this instance Officers also applies to contractors/consultants/agents working on behalf of the Council on Council business.

- ‘Orphan’ records - seeking decisions about the management of records for which there is no clear service team responsibility; for example records for activities that are no longer undertaken by the Council.

3.4 Service management responsibility

Managers at all levels are responsible for:

- Implementing and operating records management practices, covering both electronic and hard copy records, that:
    - are efficient and fit for purpose; and
    - comply with corporate information and records management policy and guidelines;
- ensuring that appropriate resources exist within the area for fulfilling the responsibilities for managing records;
- communicating local records management procedures; quality assurance of Directorate records management processes and procedures;
- ensuring that staff follow corporate procedures for the storage of hard copy records;
- ensuring that staff follow corporate procedures for the management and storage of electronic records and information ; and
- Implementation of retention schedules and ensuring regular review and authorised disposal of records is carried out.

3.5 Officer responsibilities

Everyone who creates or receives information and records is responsible for following the Council and directorate information and records management procedures.

3.6 Project records responsibility

Information and records about projects that involve two or more directorates or service teams (‘horizontal projects’) are the responsibility of the project manager.

Project managers are responsible for:

- identifying project related records and liaising with relevant local contacts
- ensuring that the records are managed efficiently and comply with our records management policy and standards;
- ensuring that there are appropriate resources within the project for fulfilling the responsibilities for managing records;
- quality assurance of records management processes and procedures within the project; and
- ensuring the appropriate disposition of project records.

4. Concepts

Underlying effective information and records management are a number of concepts that all good information and records management practices should be built on.

4.1 Authenticity

Authentic information and records can be proven to:

- be what it claims to be;
- have been created or sent by the person said to have created or sent it;
- have been created or sent at the time claimed;
- have not been tampered with; and
- be credible and authoritative so that evidence can be safely derived from it (for example to be used at the Council Tribunals, courts).

4.2 Reliability

Reliable information and records are those whose contents can be trusted as a full and accurate representation of the transactions, activities or facts they concern, and can be depended on in subsequent transactions or activities.

4.3 Integrity

The integrity of information and records refers to its being complete and unaltered.

4.4 Usability

A useable record is one that can be located, retrieved, presented and interpreted.

It should be capable of subsequent presentation as directly connected to the business activity or transaction that produced it. The contextual linkages of records should carry the information needed for an understanding of the transactions that created and used them. It should be possible to identify a record within the context of broader business activities and functions. The links between records that document a sequence of activities should be maintained.

4.5 Declaring information as a record

Whilst all records are information, not all information is a record, therefore a record needs to be identified. To decide if an item is a record, it should be examined in the context of:

- the regulatory environment;
- business and accountability requirements; and
- the risk of not keeping it.

Items should be captured as records and linked with metadata which characterise their specific business context when they:

- commit someone to do something;
- give someone responsibility for something; or

- record something that has happened.

See Appendix A for standard Central Bedfordshire Metadata fields

4.6 Version control

Sometimes successive drafts of a document must be kept to provide adequate evidence of the process e.g. substantial changes to plans during a building project.

The need to keep successive versions of items should be based on an analysis of record-keeping requirements and should be in line with corporate procedures.

4.7 Capturing records

Capturing a record means to place it in a records management system.
We need to capture items as records to:

- establish a relationship between the record, the creator and the business context that originated it (that is, why it was created);
- link it to other records; and
- ensure that appropriate audit trails are maintained

To ‘capture’ a record, explicit metadata needs to be allocated, embedded in, attached to or associated with the specific record, whatever its format. This metadata is essential for accurately re-tracing the status, structure and integrity of the record at any particular time and showing its relationships with other records.

Techniques to ensure capture of records include:

- classification and indexing which allow appropriate linking, grouping, naming, security protection, user permissions and retrieval, disposition, and identifying vital records
- arrangement in a logical structure and sequence, whether a physical (paper) file or an electronic directory, which helps with further use and reference;
- registration which provides evidence of the existence of records in a records system; and
- systems that control the actions undertaken in doing business, which:
  i. provide metadata describing the business context;
  ii. provide evidence of where a record is located;
  iii. identify what action is outstanding;
  iv. identify who has accessed a record;
  v. identify when such access took place; and
  vi. provide evidence of the transactions that have been undertaken on the record (in other words an audit trail).

See Appendix A for the list of metadata fields used by the Council

Items that have been identified as records must be captured in to a recognised Council record keeping system, which in the long term will be the Corporate EDRMS.

4.8 Registering records

The main purpose of registration is to formalise the fact that, and provide evidence that, a record has been created or captured in a records system. It also helps in retrieving the record. In a records system that uses registration processes:

- a record is registered when it is captured into the records system (this may include placing a manual record into a structured filing system or the automated registration of electronic records in an electronic record keeping system); and
- no further processes affecting the record can take place until its registration is complete. Records may be registered at more than one level (for example at the file series, file or record level) within a records system. In the electronic environment, records systems may be designed to register records automatically, in a way that is transparent to the user of the business system from which it is captured**.**

4.9 Retention

How long records are kept is determined by assessing:

- any legal requirements;
- any business requirements;
- any historical requirements
- any administrative requirements
- the risks associated with keeping or disposing of the record at any particular point in time.

Records identified for retention are likely to be those which:

- provide evidence and information about our policies and actions;
- provide evidence and information about our interaction with stakeholders;
- document the rights and obligations of individuals and organisations;
- contribute to the Council's historical record; and
- contain evidence and information about activities of interest to internal and external stakeholders.

5. Records structuring

To ensure that records are managed both effectively and consistently they need to be organised in a structured environment. Central Bedfordshire Council records are structured using a functional classification schema based upon the national 'Local Government Classification Scheme'.[2] This classification is used to support the corporate file plan.

Using a corporate records structure will enable all records, in no matter what format, to be organised consistently.

5.1 Functional records classification

This form of classification is the preferred method of organising records, as it provides a robust framework from which a solid file plan can be maintained. It

[2] http://www.esd.org.uk/standards/lgcs/viewer/viewer.aspx

uses business activities to structure the records and as such the context in which the records originated does not alter.

The classification levels
Function – The highest level of business activity in the structure, which provides a general area for the records to reside in. These are fixed corporately and are based on the Local Government Classification Scheme.

Activity – More specific, this level denotes the activity being undertaken. This level is also fixed and derived from the Local Government Classification Scheme.

Transaction – This level denotes the specific transaction taking place within the activity. Whilst there are a basic list of transactions which are fixed for the normal user, there is a degree of flexibility at this level which can be amended by the Information and Records team.

Example:

Function	Activity	Transaction
Finance	Accounts and Audit	Internal Auditing

5.2 File plans

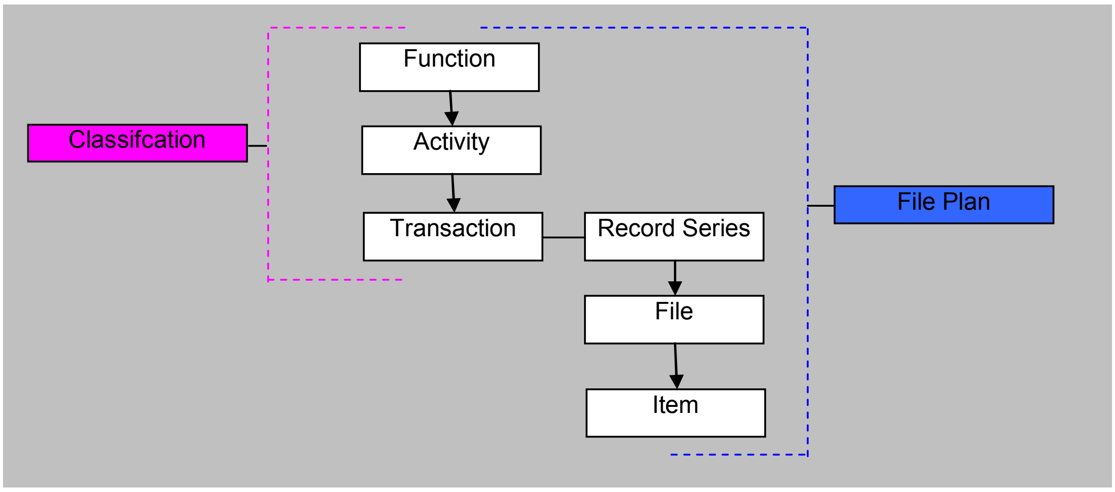
The file plan for the Council is built upon the functional classification, but with three additional layers of structure. These layers are not fixed, and provide the service teams with the ability to organise their record systems in a way that they find convenient. The additional levels are:

Record series – this identifies a group of related records that are normally used and filed together or otherwise linked, and that allow consideration as a unit for use, review, retention or destruction purposes. This level can be directly related to the Transaction in the classification scheme.

File – this identifies the actual file in which information is retained. This is the level that is generally used to manage records in a physical records system.

Item – this denotes the item within a file or a document in a records system, whilst it is possible to use this level to manage records in a physical records system it’s often not practical and is only used for individual documents such as corporate policies. However the corporate EDRMS enables records management at this level for electronic records

File Plan Structure



6. Management of physical records

It is the Council's aim to work towards a future in which the majority of Council information and records are held in digital format. However, in some cases there will be a requirement to retain physical records (such as paper and microfilm). These records must be logged on the EDRMS. This has the facility to track paper records and ensure that consistency is maintained across records of all formats.

7. Management of electronic records

All electronic records and documents will be held within a designated corporate records storage system.

EDRMS – By April 2014 all Council electronic records and documents will be held within the corporate Electronic Document and Records Management System.

Document Management Systems – there are a number of systems in use that will provide a level of document management; by April 2014 these systems will be integrated with the corporate EDRMS which will replace the document management functionality of specific systems.

Shared drive areas – there are a number of shared drives in use across the Council; these must be organised with a designated file plan in accordance with the corporate requirements. Shared drives will be phased out and replaced by EDRMS by April 2014.

8. Management of archival material

The Council is obliged by the Local Government Act 1972 to ensure that its core records are preserved indefinitely. The Council will ensure that all records designated for long term or historical preservation are transferred to a scheduled place of deposit.

9. Records storage

The Council uses a number of different storage methods for its records; this is dependent upon the following factors:

- The retention period for each record - this will determine where the record will be stored. Generally current records will be held in offices, semi-current records will be held in internal registries or commercial storage, and permanent records will be transferred to the archives.

- The format of the record – storage of physical records will depend upon the retention period (see above). Storage of electronic records will generally be on the designated electronic storage area until they are no longer required for legal, business or administrative use. At that point they will either be destroyed or transferred to the appropriate place of deposit (the Archive)

- Availability of storage space - this affects both physical and electronic records. Physical records that are still required but have no storage space will either be placed in an internal registry or file room or transferred to commercial storage. Electronic records may on occasion be transferred to alternative electronic storage areas within the EDRMS.

9.1 Commercial storage

Commercial storage of physical records will be provided using a single provider for the entire organisation. This requirement will diminish over time as more information is held electronically. The Council will ensure any commercial storage arrangements are the most cost effective, reviewed on a regular basis to ensure that they meet the Council procurement and efficiency rules.

To ensure consistency and to avoid conflicts all commercial storage arrangements will be arranged through the IRM team.

10. Scanning

In order to provide wide-ranging access to information and records the majority of physical records will be transferred into an electronic medium. This increases accessibility across the organisation and for customers who require access to Council information in an electronic format.

Document scanning will be undertaken by the corporate scanning team, and will meet the corporate standards for scanning, based on BIP 0008-1:2008[3]. This is to ensure that the records and information held in electronic format retain both their integrity and their evidential value.

Scanning is not always the appropriate solution to space shortages, as there may be legal requirements for retaining records in a physical format. No records will be destroyed post scanning unless it conforms to the corporate retention and disposal schedules, and has a signed destruction authorisation.

11. Access and security

The regulatory environment in which the Council operates sets the broad principles on access rights, conditions or restrictions that should be incorporated into records systems. These should consider legislation covering areas such as privacy, data protection, security, and freedom of information. Records may contain personal, commercial or operationally sensitive information. In some cases access to the records, or information about them, should be restricted.

Restrictions on access can be applied both within the organisation and to external users, and should reflect the legal and other rights of the Council, its stakeholders and any other persons affected by its actions.

Restricted records should be identified as such, but only where such status specifically required by a business need or the regulatory environment. Restrictions should be imposed for a stated period to ensure that the additional monitoring required for these records is not enforced for longer than needed. The need to place restrictions on access can change with time; but it should be noted that adding a restriction to a record does not necessarily prevent access to the record or the information.

The use and application of restrictions to the Council records should be carefully considered as requests for information made under the Data Protection Act and the Freedom of Information Act could still result in the information having to be released, irrespective of any restrictions previously applied.

Access status should be assigned to records, and also to individuals. Appropriate access controls ensure that:

- records are classified according to their access status at a particular time;
- records are only released to those who are authorised to see them;
- encrypted records can be read as and when required and authorised;
- records processes and transactions are only undertaken by those authorised to perform them; and

[3] Evidential Weight and Legal Admissibility of Information Stored Electronically. Code of Practice for the Implementation of BS 10008

- parts of the organisation with responsibility for particular business functions specify access permissions to records relating to their area of responsibility.

The monitoring and mapping of user permissions and functional job responsibilities is a continuing process, which occurs in all records systems regardless of format.

12. Records transfer

12.1 Physical records

External transfer - where there is a requirement for making records available to a mass audience they will, where this is practicable, be transferred into an electronic format and placed on the corporate website

When transferring records to commercial storage the records should be listed on a transfer sheet and placed in sealed boxes for transit and signed for at both ends of the transfer process.

Internal transfer - if the records are required for access by a number of individuals they should be transferred to electronic format and placed upon the corporate intranet.

When transferring between users they should be logged out and tracked using the corporate EDRMS.

12.2 Electronic records

External transfer - to ensure security and integrity, any electronic records transfer outside the Council must be done in accordance with the Data Protection Policy, the Corporate Information Governance Policy, and ICT Acceptable Use Policy.

All electronic transfers of documents with a restricted or protected security marking should be authorised by the appropriate Council officer, and must br transferred using a secure manner (i.e. suitably encrypted format or via the secure "Government Connect" network [GCsx or GC Mail]). Please contact the IRM team for specific advice.

Note:
Unauthorised use of portable storage devices is strictly prohibited

Internal transfer - for electronic records, this will be undertaken by either providing access to the specific record via the EDRMS or by placing the record on the corporate intranet. Internal transfer of records and documents via email should be avoided wherever possible.

13. Document classification

All key Council documents should be assigned with two types of Classification

Security Classification – This is mandatory for all documents (including emails) no matter their status

Functional Classification – This should be applied to all key documents of the Council

13.1 Security classifications

The purpose of security classification is to ensure that all information is secured and only accessible by the appropriate persons. All documents (including emails) must have the security classification clearly identified.

The security classification is divided into the following three categories:

Classification	**Notes**
Not Protected	A document that contains information that should or could be placed in the public domain. The majority of documents will be marked with this classification
Protected	Should be applied to a document containing information that if placed in the public domain could result in: • distress to an individual; • a breach proper undertakings to maintain the confidence of information provided by third parties; • a breach statutory restrictions on the disclosure of information • cause financial loss or loss of earning potential, or to facilitate improper gain; • an unfair advantage for individuals or companies; • prejudice to the investigation or facilitate the commission of crime; • a disadvantage to the Council in commercial or policy negotiations with others. This marking should be applied where the impact is likely to affect a limited number of individuals.
Restricted	Should be applied to a document containing information that if placed in the public domain could result in: • cause substantial distress to individuals; • make it more difficult to maintain the operational effectiveness or security; • cause financial loss or loss of earning potential or to facilitate improper gain or advantage for individuals or companies; • prejudice the investigation or facilitate the commission of crime; • breach proper undertakings to maintain the confidence of information provided by third parties; • impede the effective development or operation of government policies;

	• to breach statutory restrictions on disclosure of information; • disadvantage government in commercial or policy negotiations with others • undermine the proper management of the public sector and its operations. This marking should be applied where the impact is likely to affect a large section of the community or have a major detrimental affect on the running of Central Bedfordshire Council.

:

The appropriate classification should be added to all documents. Documents with more than a single page should have the security classification entered on each page.

The originator of the document is responsible for assigning the security classification; if unsure they should consult either their manager or the corporate Information and Records Management team.

13.2 Functional classification of documents

All key[4] documents originated by the Council must include their Functional Classification in the document appendix. This is to facilitate the placing of documents in their appropriate place in the corporate information architecture.

The classification should identify the top level function within which the document can be located. This should be added by the originator of the document in accordance with the service team file plan. If unsure the officer should consult with the Information and Records team. All documents that are created and saved within the corporate EDRMS will have a function metadata field as standard.

[4] Key Documents – these are Council documents that impact on the decision making process. This includes policies, strategies, reports, audits and accounts.

Example

APPENDIX # - Document Classification

All corporate documents are classified using the two following classification methods. For more detailed information see the Information and Records Management Policy.

#.1 Security classification

The purpose of security classification is to ensure that all information is secured and only accessible the appropriate persons. All documents (including emails) will have the security classification clearly identified.

The security classification is divided into the following three categories:

- Not Protected
- Protected
- Restricted

Refer to Information and Record Management Policy for a detailed explanation of the security classifications.

The security classification of this document is as follows:

- Not Protected

#.2 Functional classification

The purpose of Functional Classification is to ensure that all significant documents are placed in their correct position within the corporate information architecture. This is to facilitate effective management, access and disposal of information across the organisation. Each document will be marked using the corporate function (highest element of classification which describes the general area in which the document resides) under which it falls.

The functional classification of this document is as follows:

- Information Management

14. Appendix

14.1 Appendix A – Corporate Document Metadata Fields

To be inserted when finalised

14.2 Appendix B- Related Council Policies

1. Information Governance and Security Policy
2. Data Protection Policy
3. Freedom of Information Policy
4. Environmental Information Regulations Policy
5. Public Sector Re-use of Information Policy
6. ICT Acceptable Use Policy
7. Elected Members Information Policy

14.3 Appendix C - Related Statutes, Legislation and Standards

Legislation	Notes	Area of impact
The Data Protection Act 1998	The Data Protection Act requires that all personal information be handled in an appropriate way.	Access to Information Data Management Records Management Information
Freedom of Information Act 2000	Provides the legal framework around which the public are able to access information held by the Council. Section 46 – of the Freedom of information act makes it clear that in order to comply with the FoI a public body must maintain its records in a way that makes the accessible.	Access to Information/Records Management
The Environmental Information Regulations 1992	Provides the framework for public access to Environmental information of an organisation Pt2 Section 5 (4) – requires that information is accurate and up-to-date and comparable	Access to information/ Management of environmental information
Human Rights Act 1998	Article 8.1 of the European Convention on Human Rights (given effect via the Human Rights Act 2000) provides that "everyone has the right to respect for his private and family life, his home and his correspondence". However there are exemptions that override those rights, such as national security, public safety, prevention of disorder or crime, and protection of the rights and freedom of others.	The Council has a duty to abide by the human rights act and ensure that all correspondence with the Council is treated appropriately, which includes managing it in a way that will not invade the privacy of the individual.
Crime and Disorder Act 1998	Section 115 of this Act provides that any person has the power to disclose information necessary for the provisions of the Act to the police, local authorities, probation service or health authorities.	To be able to provide appropriate information the Council must not only ensure access to the information, but that the context is not lost through poor management.
Children Act	Background Every Child	Information retained in

2004	Matters: Change for Children (Dec 2004), and the draft statutory guidance on the Children Act 2004 S10 Duty to Cooperate (Dec 2004), set out clear expectations for local action to improve information sharing. It seeks to provide clarity on the legal framework for practitioners sharing information about children, young people and families; and give practitioners confidence in making decisions.	all service areas could potentially be valuable in ensuring the well being of children in the area. Therefore being able to access information from a wide range of sources across the Council is essential.
Limitation Act 1980	This act places a limit on the validity of information, therefore provides the legal framework for retention and disposal of certain documents	Retention and disposal of records, although not all records or information has a legal limitation attached.
Public Records Acts 1958 & 1967	These two acts provide the framework for the appropriate management of Public Records, these were heavily amended in with the introduction of the Freedom of Information Act	Management of Public Records
Local Government (Records) Act 1962	(10 A local Authority may do all such things as appear to Power to it necessary or expedient for enabling adequate use to be made of records under its control, and in relation to such records may particular – a) Make provision for enabling persons, with or without charge and subject to such conditions as the authority may determine, to inspect the records and to make or obtain copies thereof	Records Management
Taxes Management Act 1970	Details the requirements for managing tax records	Records retention
Local Government Act 1972	Section 224 – without prejudice to the powers of the *custos rotulerum* to give directions as to the document of any county, a principle Council shall make proper arrangements with respect to any documents, which belong to or are in the custody of the Council or any of	Records Management

	their officers	

Codes of Practice	Notes	Area of impact
FOI Code of Practice for Local Government	“1. To set out practices which public authorities, and bodies subject to the Public Records Act 1958 and the Public Records Act (NI) 1923, should follow in relation to the creation, keeping, management and destruction of their records (Part I of the Code); and 2. To describe the arrangements which public record bodies should follow in reviewing public records and transferring them to the Public Record Office…”	Access to Information

Standards
ISO 15489-1 and ISO 15489-2, 2001 ‘best practice’ for managing records in an organisation.
BIP 0008-1 a code of practice for Legal Admissibility and Evidential Weight of Information Stored Electronically.
PD 0010:1997 Principles for Good Practice for Information Management.
BS 5454:2000 Recommendations for the Storage and Exhibition of Archival Documents,
ISO 18925:2002 Imaging materials – optical disk media – storage practices
PD 0016:2001 Guide to scanning business documents
MoReq 2001 Model requirements for the management of electronic records.
BS 7799:2002 Specification for information security management
ISO-19005-1 - PDF/A-1 - Document management - Electronic document file format for long-term preservation.
Payment Card Industry (PCI) Data Security Standards
HMG Security Policy Framework
The Caldicott Report - Report on the review of patient-identifiable information

14.4 APPENDIX D - Document Classification

All corporate documents are classified using the two following classification methods. For more detailed information see Corporate Information Records Management Policy.

14.4.1 Security classification

The purpose of security classification is to ensure that all information is secured and only accessible the appropriate persons. All documents (including emails) will have the security classification clearly identified.

The security classification is divided into the following three categories:

- Not Protected
- Protected
- Restricted

Refer to Information and Record Management Policy for a detailed explanation of the security classifications.

The security classification of this document is as follows:

- Not Protected

14.4.2 Functional classification

The purpose of Functional Classification is to ensure that all significant documents are placed in their correct position within the corporate information architecture. This is to facilitate effective management, access and disposal of information across the organisation. Each document will be marked using the corporate function (highest element of classification which describes the general area in which the document resides) under which it falls.

The functional classification of this document is as follows:

- Information Management