Appendix A

Central Bedfordshire Council

Information Governance and Security Policy

Version 1.0

June 2009

Policy Governance

Accountable Director	Director of Business Transformation
Policy Author (Title)	Policy Team in consultation with ADs for: • ICT and Property • Audit and Risk • Democratic and Legal • Policy, Partnerships and Performance • SCHH - Business and Performance • Customer Services and Heads of Service for: • Countryside and Archives • SCHH – Business Systems • ICT Assurance and Applications
Approved By (Title)	
Date Approved	
Issue Date	
Review Date	
Person Responsible for Review (Title)	
Include in Publication Scheme (Y/N)	Yes
Publish to Web (Y/N)	Yes
Circulation	This policy is to be made available to all Council Officers and Elected Members There will be an ongoing professional development and awareness training available to support this document.

Policy Approval

Central Bedfordshire Council (the Council) 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 through the production of these documents and their minuted approval.

I trust that all officers, 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 Governance and Security Policy is available from the website at www.centralbedfordshire.gov.uk.

Alternatively, a copy can be obtained by writing to the Principal Information and Records Officer at:

Central Bedfordshire Council

Priory House

Chicksands

Shefford

SG17 5TQ

Contents

1. **Introduction**
2. **Purpose and Scope**
3. **Responsibilities**
4. **Legislation and Standards**
5. **Policy Framework**
6. **Annex A - Document Classification**

1. INTRODUCTION

This policy sets a new culture of information use in Central Bedfordshire, with the Council operating to a default principle of its information being open, transparent and in the public domain – except where for legislative reasons access to / use of information is restricted.

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 aim to be open in its provision of information to the public and stakeholders wherever possible, on which much confidence and trust is founded, with its obligations and duties around confidentiality and data protection. This balance requires the Council to create and manage all records efficiently, to make them accessible when needed, to protect and store them securely and to dispose of them safely at the appropriate time.

Effective information management will bring many benefits to the Council by facilitating and supporting more efficient working, better decision making, improved customer service and business transformation.

A key component of information management is effective information governance and security, which is the subject of this policy document. The public sector in the UK has had a number of high profile information losses and breaches resulting in a significant loss of confidence and trust in the public sector's handling of information. There is now a greater reliance on electronic information and records, over the traditional paper mediums, and this is resulting in a more information centric society. As a result expectations are changing and the rules and standards are being tightened to ensure that appropriate levels of security are applied where necessary.

This policy is part of a suite of information management policies which have been adopted by the Council and which apply to all officers (including all agency workers and contractors). These are:

- Data Protection Policy (in response to Data Protection Act 1998);
- Freedom of Information Policy (in response to Freedom of Information Act 2000);
- Environmental Information Regulations Policy (in response to Environmental Information Regulations 2004);
- Re-use of Public Sector Information Regulations Policy (in response to Re-use of Public Sector Information Regulations 2005);
- ICT Acceptable Use Policy;
- Information and Records Management Policy.

For Elected Members a Members' ICT Provision Policy was agreed by the Executive in May 2009. Specific polices for Members will be developed in respect of ICT Acceptable Use, Information and Records Management and Data Protection.

Many elements of these policies will require significant changes to the Council's working culture and practices and will be supported by an extensive awareness raising and training programme in relation to information management responsibilities.

The aims of this suite of policies are to preserve:

- **Confidentiality** – confining the access to data to those with specific authority to view it.
- **Integrity** – safeguarding the accuracy and completeness of information and ensuring the correct operation of all systems, assets and networks.
- **Accessibility** – ensuring that information is available and delivered to the right person, at the time when it is needed.
- **Authenticity** – ensuring information and records are credible and authoritative.
- **Reliability** – ensuring information and records can be trusted as a full and accurate representation of the transactions, activities or facts.

Objectives

The objectives of this Information Governance and Security policy are for the Council to achieve:

- **Openness** - by making information more available to benefit the whole community
- **Legal Compliance** - by adhering to the appropriate legislative requirements to minimise the risk to public information and monies through inappropriate use.
- **Information Security** - by ensuring information is protected against unauthorised access and potential misuse.
- **Information Quality Assurance -** by ensuring information is accurate, authentic and reliable.

2. PURPOSE AND SCOPE

The purpose this policy is to set out the controls and requirements that will operate to protect the wide range of information that is generated, shared, maintained and ultimately destroyed or archived.

This policy applies to:

- all employees of the Council
- all elected members of the Council
- all employees and agents of external organisations who in any way support or access any Council information system

and information which is:

- stored on computers

- transmitted across networks
- printed out and/or filed in some form
- written on paper and/or filed in some form
- sent by fax
- stored on tapes and disks
- spoken in conversation e.g. by telephone
- sent via E-mail
- stored on databases
- held on microfiche.

3. RESPONSIBILITIES

The ultimate responsibility for ensuring open and transparent use of the Council's information rests with the chief information officer (the Director of Business Transformation).

Ultimate responsibility for security rests with the Chief Executive of the Council, with delegated authority to the Director of Business Transformation acting as the Senior Information Risk Owner (SIRO).

The SIRO will chair the Information Governance Steering Group (IGSG) who are responsible for initiating, developing and monitoring the delivery of information governance in Central Bedfordshire Council as part of the Council's corporate information management.

On a day-to-day basis the Information Governance and ICT Assurance leads will be responsible for managing the policy and working with service managers to ensure robust security procedures are in place and are being complied with. This includes ensuring that permanent and temporary officers and contractors are aware of:

- the information governance and security policies applicable in their work areas;
- their personal responsibilities for information governance and security; and
- how to access advice on information governance and security matters.

The Senior Information Risk Owner (SIRO) and the Caldicott Guardian[1] are responsible for ensuring that information governance is embedded into the organisation to ensure that the potential risks to corporate information and records are mitigated.

The Principal Information and Records Officer will take day-to-day responsibility for developing, monitoring and overseeing the implementation of the corporate information and records management policies, procedures and guidelines and providing the mechanisms for supporting access to information compliance.

[1] Caldicott Guardian – specific role required to oversee the management of the Council's health and social care information and record holdings.

4. LEGISLATION AND STANDARDS

The Council will comply with all relevant UK and European legislation and industry standards. This requirement is devolved to employees and agents of the Council who may be personally accountable for any breaches of information security for which they may be held responsible. The principal **legislation** to which the Council will comply is:

- Children Act, 2004
- Computer Misuse Act, 1990
- Copyright, Designs and Patents Act, 1998
- Crime and Disorder Act, 1998
- Data Protection Act, 1998
- Data Protection (Processing of Sensitive Personal Data) Order, 2000
- Environmental Information Regulations, 1992
- Freedom of Information Act, 2000
- Health and Safety At Work Act, 1974
- Human Rights Act, 1998
- Limitations Act, 1980
- Local Government Act, 1972
- Re-use of Public Sector Information Regulations, 2005
- Regulation of Investigatory Powers Act, 2000
- Taxes Management Act, 1970.

The principal **standards** are:

- **Payment Card Industry Data Security Standard (PCI DSS)**

The Council has defined responsibilities to protect cardholder data and the supporting environment and infrastructure

- **Government Connect Code of Connectivity (CoCo)**

The Council will ensure it meets the mandatory security requirements defined in the CoCo agreement.

- **HMG Security Policy Framework (SPF)**

Although aimed primarily at Government departments and agencies in supporting their protective security and counter-terrorism responsibilities, the SPF has wider application in supporting data protection and commercially sensitive information held by local authorities.

5. POLICY FRAMEWORK

Information security risk assessment and management

The Council will promote the introduction and embedding of information security risk assessment and management into the key controls and approval processes of all its major business processes and functions to safeguard the interests of service users, officers and the Council itself.

The aim is to mitigate risk by providing the means to identify, prioritise and manage all Council activities in respect of high risk commercial and sensitive personal information and records but not at the expense of the health and safety of an individual or providing openness to information wherever possible.

Information risk assessment and management is an essential element of broader information governance and is an integral part of good management practice. The intent is to embed information risk management in a very practical way and not to impose risk management as an extra requirement.

Information security awareness training
All officers and members will be given information governance and security awareness training. Appropriate officers will receive tailored training relevant to their roles and the systems they use including any requirements to achieve compliance with external standards.

Job descriptions and contracts of employment
All job descriptions will include a general statement about responsibilities for information and data collection. Where officers have defined responsibilities specific to their job role, these will be included in and regularly reviewed as part of the performance and development review (PDR) process.

As part of their contract of employment all officers will receive a copy of the ICT Acceptable Use Policy and confirm their adherence to that policy. Induction will cover the fundamental expectations in relation to information management responsibilities including security.

Security control of information assets
All major information assets will be identified on corporate information asset registers and have a designated Information Asset Owner (IAO), who will make decisions about the protection of those assets that are consistent with this policy and/or any other applicable legislation.

In order to minimise loss of or damage to assets and/or information, equipment will be appropriately protected from security threats and environmental hazards and security marked/tagged using the Council's standard procedure.

Access management
Access management underpins many of the controls designed to protect systems, data, offices and infrastructure from unauthorised access attempts – including physical access to information whether they are in the corporate computer systems, held in offices, records stores, the corporate archive or commercial storage.

A range of controls will be in place to ensure that access to information, information processing facilities and business processes are controlled on the basis of business need and security requirements.

The types of controls to be put in place are as follows:

- **Physical access controls**
  Only authorised personnel who have an identified business need will be given access to restricted areas containing information systems. The IAO, working in collaboration with other officers such as the Information Security and/or Information Governance Lead, will determine the rules for granting access to these areas.
- **Information access control**
  Access to systems (regardless of medium) containing information shall be restricted to authorised users who have business need to use the systems. Each system will have a security protocol that includes rules about access control. These rules will cover matters such as:
  - secure log on procedures
  - identifying users
  - password management system
  - use of system utilities
  - session time-out
  - limitation of connection time
  - information access restrictions
  - sensitive system isolation
  - privilege management
  - unattended user equipment and data.

- **Equipment Security**
  In order to minimise loss of, or damage to, all assets, equipment shall be physically protected from threats and environmental hazards.

Information security events and weaknesses
All information security events and suspected weaknesses are to be reported to the appropriately designated officer(s) to ensure they are dealt with in a timely and effective manner.

All information security events will be investigated (overseen by the SIRO and IGSG) to establish their cause and impacts with a view to considering action to avoid the occurrence of similar events.

Protective marking scheme
Best practice in information assurance requires information to be categorised and identified using an appropriate scheme (known as a protective marking scheme).

The Council has adopted and will work towards implementing the following levels of security classification:

- Not Protected – information that should or could be placed in the public domain.

- Protected – should be applied where the release of information will impact upon a limited number of individuals.
- Restricted – should be applied where the release of information will impact on a large section of the community.

Full details of this scheme are in the Information and Records Management Policy.

Network security
The secure management of networks, which may span organisational boundaries, requires careful consideration of the legal implications of dataflow, monitoring and protection. Additional controls may also be required to protect sensitive information passing over public networks.

The key general principles that all system users need to comply with are as follows:

- The Council will use software countermeasures and management procedures to protect itself against the effects of malicious software. All system users will be expected to co-operate fully with this requirement.
- Users must not install software on the Council's systems and/or infrastructure without permission from ICT. Users breaching this requirement may be subject to disciplinary action.
- Devices containing software or data from external sources, or that have been used on external equipment, require the approval of ICT before they may be used on the Council's systems. Such media must also be fully virus checked before being used on the organisation's equipment. Users breaching this requirement may be subject to disciplinary action.

Laptops and removable media
Modern working practices create a demand for the widespread use of laptops and removable media. Although these offer considerable advantages to business efficiency and practice they also pose particular risks that need to be managed. A number of controls will be put in place to govern the use of laptops and removable media. These will cover matters such as:

- the configuration, identification, registration, storage and disposal of the machines themselves and the regular review of the Council's laptop holdings
- the responsibilities placed on users (and any authorisations required) in respect of:
    - the processing, storage, back up and disposal of information
    - the restriction on the use of removable media (such as CDs and DVDs, memory sticks and digital cameras) to the devices which have been provided by the Council for Council business
    - the day to day security of Council laptops and their information, including in particular the risks of using laptops off site and the precautions that should be taken to mitigate such risks
- remote access from a laptop to Council information systems.

Appropriate guidance and training will be given to users of laptops to support the implementation of controls.

System change control
Network and system software, hardware and operating procedures are subject to regular change. Any changes will be subject to a strict change control regime to ensure that all changes are controlled and approved.

Information sharing
The sharing of sensitive information between Central Bedfordshire Council and other organisations will be governed by clear and transparent procedures that satisfy the requirements of law and best practice guidance and will be defined within agreed information sharing protocols and agreements.

The principal mechanism for sharing information with central government agencies will be established through the use of Government Secure Extranet (GSx).

Locally, data sharing arrangements will be in accordance with the Bedfordshire and Luton Information Sharing Protocol details of which are in the Council's Data Protection Policy.

Safe haven guidelines
Safe havens are designated areas where sensitive and personal information can be transported and distributed safely and securely to protect service user confidentiality. Officers will be provided with guidance on the use of safe havens for distributing information via faxes, telephone, post and electronically.

Information and records management
The Council will ensure there are procedures in place to prevent the creation of duplicate records and/or filing systems, especially personal filing systems. There will also be procedures to maintain the integrity of electronic and paper-based information systems so as to minimise general information risk. This will include officers checking details held on key systems with the source e.g. with the person who supplied the information. Officers will receive guidance on good practice and improvements in local information and records management practices including moving towards more electronic forms of filing and management of records.

- **Information and data collection activities**
  The Council will ensure that there are documented procedures in place covering all key information systems. These procedures will allow for spot checking of data collection activities, and for ensuring that all entries have been recorded in accordance with the agreed information collection policies and procedures.

- **Rationalising databases/data sets**
  The Council will endeavour to minimise the number of databases and datasets held, by the use of the corporate Enterprise Content Management (ECM) System, to facilitate the management of datasets. However where it is appropriate that separate databases/datasets are held there will be control mechanisms in place to ensure that any common data is consistent, accurate and up to date.

- **Correction of errors and omissions**
  The Council will ensure that local procedures require services to regularly validate information and data within agreed timescales. This will include reconciliations between electronic and paper-based records to ensure that events have not been missed and, if appropriate, contacting the person who supplied the information.

  The correction of errors and omissions arising from validation, or from internal or external audits, will be carried out according to agreed timescales and confirmation of such recorded.

  The cause(s) of errors and omissions will be established and followed up with officers concerned so that lessons learned are passed on and repetition avoided. Where ongoing and regular problems are identified, the resolution of these will be addressed through further training and supervision.

- **Information, records and data auditing**
  The Council will ensure that there is an established internal and external audit programme in place covering all key systems.

  This timetabling and focus of this programme will be based on an assessment of risk to key information systems, or may be influenced in the event of an information-related security incident and the findings of an internal or external audit or inspection. The SIRO and IGSG will be involved in any agreements regarding the execution of the audit programme where a security incident has occurred.

  The Council will also ensure that it has a robust system in place for identifying its information and records series. This will be achieved by carrying out regular information and records audits and ensuring a consistent approach is adopted as outlined in the Information and Records Management Policy.

Information quality assurance

Responsibility for information quality and records management will be allocated appropriately throughout Central Bedfordshire Council and formalised in all relevant job descriptions.

Business continuity and disaster recovery plans

The Council will ensure that business impact assessment, business continuity and disaster recovery plans are produced for all critical information and records, and their applications, systems and networks.

Monitoring and compliance assurance

Compliance with this policy is mandatory for everyone included within its scope. Where instances of non-compliance are suspected, established disciplinary measures will be invoked and action taken dependent on the findings of the investigatory process.

Compliance audits will be undertaken and findings and recommendations reported to the IGSG, who will ensure that significant risks and issues are addressed in the most appropriate manner.

6. ANNEX A

DOCUMENT CLASSIFICATION

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

Security classification

The purpose of security classification is to ensure that all information is secured and only accessible to appropriate persons. All documents (including emails) will have the security classification clearly identified unless it is categorised as 'Not Protected', the default position for openness.

The security classification is divided into the following three categories:

- Not Protected
- Protected
- Restricted

(For a detailed explanation of these security classifications see the Information and Records Management Policy.)

The security classification of this document is:

- Not Protected

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:

- Information Management