Central Bedfordshire Council

Information Governance Framework

Version [1]

Document sign-off

Owner	Role	Signature	Date	Version
Richard Ellis	Director of Business Transformation - Senior Information Risk Owner			

Approval History

Version No	Approved By	Approval Date	Comments
			e.g. approved at IGSG meeting on dd/mm/yyyy
v			

Revision History

Version No.	Revision Date	Summary of Changes	Author
v0d8	14/01/2010	1st draft issued to IGSG for comment	Dave Jones
v0d9	08/03/2010	2nd draft issued to IGSG for comment ▪ added target completion dates for incomplete policies, ▪ completed section on Legal Service, ▪ added guidance on IGF roll out approach including readership and training needs.	Dave Jones
v0d10	05/07/2010	3rd draft issued to EM and CJ final comments prior to sign-off. ▪ ,added reference to the Human Rights Act 1998, ▪ added reference to RIPA 2000, ▪ updated wording of data quality and performance governance controls, ▪ removed IGSG membership structure chart, ▪ re-sequenced Appendices ▪ corrected typos.	Dave Jones
v1	06/08/2010	Accept changes recommended by Elaine Malarky	Dave Jones

Document Author

Version	Authors	Role
v0d8	Dave Jones	ICT Service Assurance & Improvement Manager
v0d8	Rob Hutton	Principal Information Risk Officer
v0d8	Peter Badger	ICT Security Manager
v0d9	Dave Jones	ICT Service Assurance & Improvement Manager
v0d10	Dave Jones	ICT Service Assurance & Improvement Manager
v0d11	Elaine Malaky	Head of Planning and Programme Management
v1	Dave Jones	ICT Service Assurance & Improvement Manager

Document Governance

Next Review Date	This document will be reviewed annually or inline with changing business requirements. This process will be audited as per the Information Security Management Systems audit schedule.
Include in Publication Scheme (Y/N)	
Publish to Web (Y/N)	No, Intranet only
Circulation	This framework 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 framework.
Information Classification	**NOT PROTECTED**

The current version of the Central Bedfordshire Council's Information Governance Framework is available from the CBC intranet at *<insert hyperlink here>*

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

Table of Contents

1 Introduction

This document (the Central Bedfordshire Council Information Governance Framework) forms the basis of how Information Governance is structured at Central Bedfordshire Council (CBC), how Information Governance related policies, procedures and guidelines are structured and how the various Directorates and Services are aligned to support Information Governance at CBC. Appendix A contains a diagram of the Information Governance Framework.

Information Governance within CBC is overseen by the Information Governance Steering Group. The Terms of Reference for the Information Governance Steering Group (IGSG) can be found on the CBC intranet. A list of current members of the IGSG can be found on the Information Management pages on the CBC intranet.

Information Governance is many things to many people. Central Bedfordshire Council (CBC) views this as:

- the cornerstone of information management and information security management.
- key to ensuring the Central Bedfordshire Council comply with current legislation, regulation and best practice appropriate to local government, in relation to the creation, handling, storage, security and processing of information.
- allows organisations and individuals to ensure 'Protected' and 'Restricted' information is appropriately identified and dealt with legally, securely, efficiently and effectively.
- provides a platform to initiate User Awareness and training programmes to ensure staff, contractors and 3rd parties are aware of their Information Governance responsibilities.
- The Information Governance Framework (IGF) sets out the structures that are in place to govern the Information Management and the Information Security Management processes including; the policies and procedures that must be put in place to safeguard the council.
- The IGF clearly states the 'Standards' that Central Bedfordshire Council will adopt or work towards adopting to continually improve Information Governance.
- Clearly defines the measures that the council has adopted (KPIs and PI) to report the effectiveness of the Information Governance process.

Information Governance has eight fundamental aims:

- To ensure accountability, the Council will ensure that there is a senior executive who will oversee the information management approach and delegate programme responsibility to appropriate individuals, adopt appropriate policies and procedures to guide personnel, and ensure programme audit ability.
- To ensure integrity of information, an information management programme will be constructed so that information and records generated or managed by, or for, the Council have reasonable and suitable guarantee of authenticity and reliability.
- To ensure that information is protected, the information management programme will ensure that the appropriate level of consideration is given to provide a reasonable level of protection to all information and records especially those that are identified as Protected, Restricted, or are essential to business continuity.
- To ensure that information held meets relevant compliance requirements - the information management programme will be constructed to comply with applicable laws and other binding authorities, as well as the Councils policies.
- To ensure that information is available, the organisation will maintain information and records in a manner that ensures timely, efficient, and accurate retrieval of needed information.
- To ensure that information is transparent, the processes and activities of the Council's information management programme will be documented in an understandable manner and be available to all personnel and appropriate interested parties.
- To ensure that information is retained consistently the Council will maintain its records and information for an appropriate time, taking into account; legal, regulatory, fiscal, operational, and historical requirements.
- To ensure that any disposal of information is carried out correctly, the Council will provide secure and appropriate arrangements for information that is no longer required by any applicable laws and or the council's policies.

The Information Governance framework encompasses:

- Data Protection Act 1998
- Access to Information legislation
    - Freedom of Information Act 2000, including the Council's 'Publication Scheme'
    - Public Sector Information Regulation 2005
    - Environmental Information Regulation 2004

- Regulation of Investigatory Powers Act 2000,
- Human Rights Act 1998, article 8,
- Information and Records Management
- Information Security Management System
- Information Governance Management

2 Plan/Do/Check/Act (PDCA) Model

The following review model has been adopted by Central Bedfordshire Council to ensure continuous improvement of the Information Governance Framework:

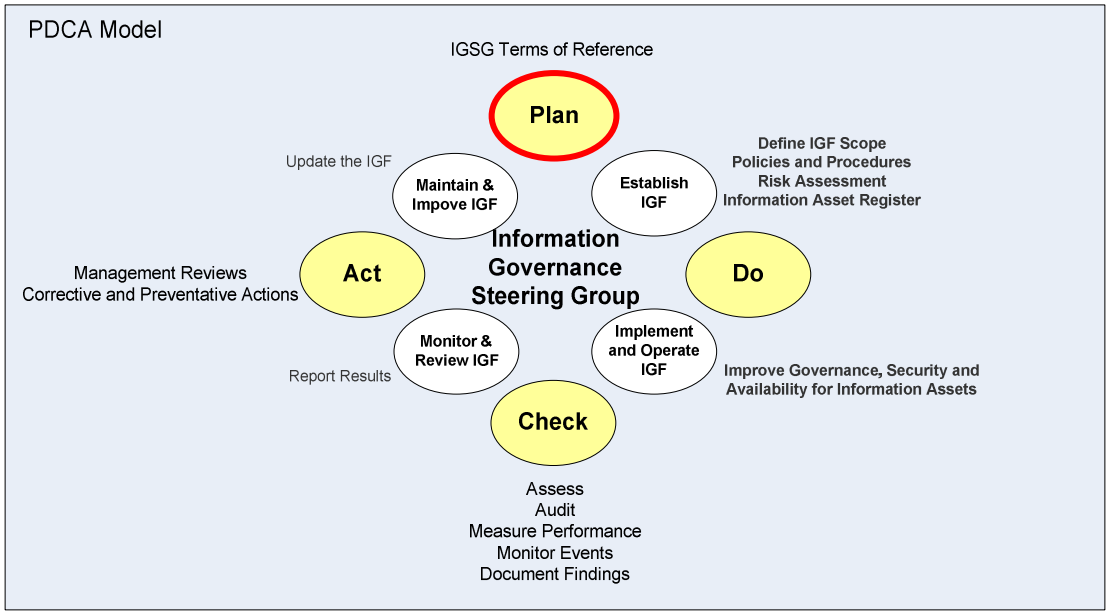

Figure 1 – PDCA Model

Plan
(establish the IGF)

Establish policies, objectives, targets, processes and procedures relevant to managing risk and improving information governance to deliver results in accordance with CBC's overall policies and objectives.

Do
(implement and operate the IGF)

Implement and operate policies, controls, processes and procedures.

Check
(monitor and review the IGF)

Assess and, where applicable, measure process performance against policies, government performance indicators, objectives and practical experience. Report the results on a monthly basis to management for review.

Act
(maintain and improve the IGF)

Take corrective and preventive actions, based on the results of the management review, to achieve continual improvement of the information governance framework.

3 Role of the Senior Information Risk Officer (SIRO)

The SIRO has been appointed by the Chief Executive.

The SIRO is fully aware of how the strategic business goals of the Council may be impacted by information risks.

The SIRO acts as an advocate for information risk on the Council's Management Team (CMT) and in internal discussions, and provides written advice to the Chief Executive Officer on the content of their Annual Governance Statement in regard to information risk.

Working within a simple governance structure, with clear lines of ownership and well defined roles and responsibilities, the SIRO provides an essential role in ensuring the identified information security threats are followed up and incidents managed.

The SIRO also ensures that the Board and the Chief Executive Officer are kept up-to-date on all information risk issues.

The SIRO is responsible to the Board for ensuring that all Information risks are recorded and mitigated where applicable. The SIRO is responsible for ensuring that all record management issues (including electronic media) are managed in accordance with this policy.

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

The role is supported by Information Asset Owners (IAOs)[1], the Risk Manager; the Principal Information Records Officer, the ICT Security Manager and the Caldicott Guardian, although ownership of the Information Risk Policy and risk assessment process remains with the SIRO.

Please refer to Appendix B for a description of the Information Asset Owner (IAO's) role.

The SIRO is responsible for the appointment and management (in terms of information assets) of the IAO's. Information Asset Owners are senior individuals involved in running the Council. Their role is to understand and address risks to the information assets they or their team(s) 'own' and to provide assurance to the SIRO on the security and use of those assets.

The IAOs (in consultation with the SIRO) are responsible for appointing Information Asset Administrators (IAAs). Information Asset Administrators ensure that policies and procedures are followed, recognise actual or potential

[1] The Council has determined that the IAOs role will be at Head of Service (HoS) level within the organisation.

security incidents, consult their IAO on incident management, and ensure that information asset registers are accurate and up to date.

4 Structure of the Information Governance Framework

The main functional areas within CBC that fall within the framework are:

- Information & Records Management
- Performance Management and Data Quality
- Information Security Incident Management
- ICT Services
- Properties & Facilities Services
- Human Resources Services
- Risk Management, including Audit and Assurance
- Legal Services

The Information Governance Framework is guided by the Council's Corporate Strategy and Directorate Plans.

Measurements of effectiveness of every relevant function and control within the overall Information Governance Framework, will be through KPIs and PIs which will be reported upon on a regular basis. A programme of continuous improvement will also be implemented.

An audit and assurance programme will be devised and implemented to ensure the ongoing effectiveness and compliance of the Terms of Reference, this framework document and best practice standards, such as ISO27001:2005, BS15489 and BS25999.

4.1 Information & Records Management

Having accurate, relevant and accessible information, both current records and archives, is vital to the efficient management of the Council, which values recorded information as an important corporate asset. The Council must meet its statutory obligations in this area, making 'proper arrangements' for its records, both for its own good governance but also so as to provide the public with access to information. In doing this it will seek to be open and responsive with access to information whilst meeting its duties of confidentiality in relation to personal and commercially sensitive records and information.

This requires the Council to create and manage all its recorded information, irrespective of its medium and position in its managed lifecycle, efficiently, make them accessible when needed, protect and store them securely and dispose of them safely at the appropriate time.

In relation to its semi-current hard copy recorded information and archives, these functions are provided by Bedford Borough Council through a Service Level Agreement (SLA) following Local Government Reorganisation and the creation of Central Bedfordshire Council in 2009.

The Bedfordshire and Luton Archives and Records Service, the subject of the SLA, is a scheduled Place of Deposit for Public Records and also provides a joint arrangement service to Luton Borough Council for both Archives and Records Management.

Please refer to Appendix C for a list of relevant Information & Records Management policies, procedures and guidelines.

The Council (seeks to at all times comply) complies with all relevant legislation (refer to Appendix D) 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). In respect of the Service Level Agreement for the provision of Archives and Records Management Services discharged by Bedford Borough Council are concerned, this involves an agreed set of arrangements for governance, monitoring, performance, issue management, and compliance and a series of scheduled Service Level KPIs – see below.

Service Level PI ref.	Service Key Performance Indicator (KPI)
SER1	Overall performance in national assessment by The National Archives – this includes the following areas: governance, documentation of collections, access and outreach services, preservation and conservation, buildings, security and environment
SER2	Charter Mark accreditation
SER3	Customer satisfaction in national surveys of users
ARR1	Performance in national assessment by The National Archives
ARR2	National accreditation as Place of Deposit for Public Records
ARR3	Volumetric intake of corporate records from each partner
ACC1	Visitor provision – performance against Service Charter targets
ACC2	Remote enquiry provision (written)
ACC3	Remote enquiry provision (telephone)
ACC4	Website pages
ACC5	Website hits
ACC6	Retro-digitisation of lists and related indexing

ACC7 ACC8	Website content development
ACC9	Outreach work
ACC10	Information management • Electronic Records Management linked with… • Digital Preservation

4.2 Performance Management & Data Quality

Central Bedfordshire Council takes the quality of its performance data very seriously. We aim to ensure that our decision makers are provided with information that is fit for purpose and is used to support the decision making process.

Having reliable, accurate and timely information to support decision making and manage services is essential. Data must be fit for purpose and represent an organisation's activity in an accurate and timely manner. This will give us confidence in the decisions we make as a result.

We spend a great deal of time and money on the activities and systems involved in collecting and analysing the data that underpins information at the Council. It is therefore absolutely essential that we should have confidence in the data we produce as increasing reliance is placed on the information that comes from it and it enables us to demonstrate our improvement. It is essential that the responsibility for data lies with all staff that input, store, retrieve or otherwise manage data to ensure that it is of the highest quality.

Our vision for data quality is that we get it right first time, every time. This is vital to the delivery of our Strategic Plan and the monitoring of the actions and target milestones contained in it. We must continue to be robust about demonstrating improvement in our performance as it will give us a level of confidence when providing this information to Government auditors and inspectors and other external assessors.

Data quality in relation to Central Bedfordshire Council's performance indicators is monitored and reported regularly during the year and any concerns regarding the quality of any performance data will be addressed and resolved.

Data used for performance information is subject to proportionate verification to check accuracy, validity, reliability, timeliness, relevance, completeness and security. This underpins the Data Quality Strategy.

Please refer to Appendix E for a list of relevant Performance Management & Data Quality policies, procedures and guidelines.

4.3 Information Security Incident Management

The purpose of information security incident management is to ensure information security events, and weaknesses associated with information systems, are communicated in a manner allowing timely corrective action to be taken, and to ensure a consistent and effective approach is applied to the management of all reported information security incidents.

Formal information security event reporting and escalation procedures are in place. All employees, contractors and contracted third parties are aware of the procedures for reporting information security incidents and potential weaknesses that could have an impact on the security of Council's information assets.

All employees, contractors and contracted third parties are required to report any information security incidents and weaknesses as quickly as possible to the ICT Service Desk.

Responsibilities are assigned and procedures are in place to handle information security incidents and to assess weaknesses effectively once they have been reported. A process of continual improvement is applied to; protective monitoring, incident evaluation and response, incident containment, eradication and recovery and the overall management of information security incidents.

Please refer to Appendix F for a list of relevant information security incident management documents, procedures and guidelines.

4.4 ICT Service

Central Bedfordshire 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 its stakeholders.

The purpose of the Central Bedfordshire Council ICT Acceptable Use Policy (CBC ICT AUP) and other ICT security policies, standards and baselines which govern how the Council's technology is deployed and managed is to ensure that information assets are reliably protected. The policies, standards and baselines apply to all employees, members, contractors and third parties at any location with access to CBC's computing resources and information.

ICT Security and Information security is the responsibility of every employee, member, contractor and authorised 3rd party.

The Council reserves the right to monitor ICT use for compliance with their ICT security policies. Consequences of ICT security policy violations may lead to disciplinary action against employees and the termination of contracts under which contractors and third parties provide services to CBC.

Please refer to Appendix G for a list of relevant policies, procedures and guidelines which when combined govern CBC ICT Systems and their use. These are categorised into:

- ICT End-Users Security Policies, such as the ICT Acceptable Use Policy and Members ICT Acceptable Use Policy; and
- ICT Security Management policies (which govern how ICT Services are implemented and managed)

4.5 Properties & Facilities

The Properties and Facilities service has responsibility for delivering various services to the Council in relation to Information Governance, in particular providing a secure environment in which Council staff and members can work.

The Service ensures that each council building is appropriately physically secured and ensures safety systems are in place and operational, including fire alarms.

At the Council's main buildings access control systems have been implemented to control who has access to various parts of each building and at which times of day they have access. The Service issue security passes, for the access control system, to permanent staff and authorised contractors and will revoke access for people when they leave. The Service also provides reception security staff that sign visitors in and out of the buildings and issue visitor passes.

The Service facilitates the provision of additional levels of security to ensure specific rooms are appropriately protected, for example. ICT data centre rooms.

The Properties and Facilities service are also responsible for the implementation, management and operation of surveillance systems (e.g. CCTV), where there is a business need and for ensuring buildings are maintained at an appropriate level.

Please refer to Appendix H for a list of relevant policies, procedures and guidelines.

4.6 Human Resources Service

The Human Resource Service provides a range of services to support the Council directorates to achieve their goals, bringing the Council's vision to life. These include; recruitment, learning & development, workforce planning, employee relations support, provision of management information, corporate induction and setting HR policies which facilitate the retention of the right people to deliver a first class service to the residents of Central Bedfordshire.

To help protect the Council's information assets, all employees must clearly understand their security responsibilities. For some roles, these should be

addressed in the job description, but in general terms, employees will sign up to their responsibilities through their terms and conditions of employment. HR must ensure every employee has signed a contract of employment and that all employees that use ICT Services, in their role, additionally sign a declaration to comply with CBC's ICT Acceptable Use Policy (AUP).

For new starters, HR are responsible for ensuring that employees, contractors and third party users are recruited through a robust agreed process, are issued with a contract of employment, and associated ICT AUP (where appropriate). Additionally, corporate and local induction will help to ensure that all new starters clearly understand their responsibilities.

To help reduce the risk of theft, fraud, misuse of Council facilities or reputational damage to the Council and to help ensure that candidates are suitable for the role they are being recruited for, all prospective employment candidates, contractors and third party users must be appropriately background checked by HR prior to commencing their employment with CBC. The level of background checks required for each role is clearly documented in the recruitment procedures, and the process is routinely audited.

The HR team produces regular and ad hoc management information for managers, and is responsible for the accuracy, relevance and validity of that information.

HR has clearly documented procedures for managing processes in relation to starters, leavers and changes, and the associated work relating to payroll. In relation to leavers, there is a process that managers use to ensure that CBC equipment /assets, ID badges are returned, and that system access rights are removed.

HR has established policies e.g. disciplinary procedure, to ensure, in relation to information governance (in this case), that breaches in information governance or security arrangements can be dealt with appropriately. HR must also provide appropriate guidance and training to all managers to ensure the disciplinary procedure is applied consistently across the Council.

HR is also responsible for setting and overseeing policy to govern employees' behaviour whilst employed by CBC. Please refer to Appendix I for a list of relevant policies, procedures and guidelines to facilitate the governance of employees.

4.7 Risk Management

CBC acknowledges its ongoing responsibility to afford a high priority to the development and implementation of robust and integrated processes that will ensure that risks are identified, assessed, prioritised, managed and recorded in a consistent and holistic way, and wherever reasonably practicable, eliminated or controlled.

CBC has a Corporate Risk Management Strategy that ensures that all parts of the organisation identify and prioritise risks, and that the strategic, directorate and service level Risk Register capture risks and have mechanisms to determine acceptable levels of risk and to describe, implement and monitor mitigating and remedial actions.

CBCs Corporate Risk Management process and strategy is overseen by the Corporate Risk Management Group which is mandated to meet at least four times a year. Additional meetings can be held if considered necessary.

Please refer to Appendix J for a list of relevant strategies, policies, procedures and guidelines.

Audit & Assurance

It is the policy of Central Bedfordshire Council that aspects of the Information Governance Framework will be subject to an internal audit from time to time. Due to the size of the Council and the number of sites that it operates from this will be conducted on a rolling basis, with a number of areas being selected to be audited each year, using a risk based approach. This will help ensure that not only policies and procedures are being applied appropriately but also that changes in best practice are implemented and policies and procedures regularly reviewed and updated.

The Internal Audit Service has developed and maintains an Audit Plan, which aims to cover major risk aspects of compliance with CBC's information governance policies.

Sites and/or aspects of the IG Framework may receive an audit visit more than once in the three year period where there are deemed to be critical functions or where previous audits have revealed serious or numerous non conformities to recognised standards or best practice.

Additionally, aspects of ICT Security will be audited (by Internal Audit, external consultants etc) as part of Central Bedfordshire Council's ongoing audit process.

In addition to formal audit checks, the ICT Service works with external agencies each year to conduct assessments for compliance to the following standards and codes of connection:

- Government Connect Code of Connection (GCSx CoCo)
- Payment Card Industry Data Security Standard (PCI-DSS)

Please refer to Appendix J for a list of relevant policies, procedures, guidelines and reports which contribute to CBC Information Governance.

4.8 Legal Service

The Legal Services team do not directly provide policies, procedures and guidelines with respect to CBC information governance management. They do however provide a consultative service to all directorates across the council,

and will apply their legal knowledge to contribute to Council policy when requested.

5 Guidance on Implementation

5.1 Information Governance Framework - Target Audience

The Information Governance Framework must be understood by all information asset owners and also all officers of the Council that have supervisory duties, within Services that handle sensitive (Protected or Restricted) data which if mishandled could cause damage to the council.

The Information Governance Framework is an over-arching framework that aims to pull together the various components that contribute to Information Governance across the Council, so that information asset owners and line managers have a single source of reference regarding CBC's Information Governance policies.

The Information Governance Framework document is not a protected document and is accessible on the CBC intranet.

5.2 Information Governance Framework - Awareness Training

While safeguarding the Council's information is every council employee, contractor and member's responsibility, specific training on the Information Governance Framework is not required for all staff.

Programmes of awareness and training are run, from time to time, within each of the Services that contribute to CBC's Information Governance policies, for instance,

- HR regularly run training and briefing sessions on HR policies and procedures for new line managers and refresher sessions for existing managers (where required). These sessions are normally scheduled through the Academy website and are regularly advertised within Be Inspired.

- Staff that handle information and/or use ICT systems will receive regular awareness training, in the form of ICT AUP acceptance or Information Security awareness training (planned from summer 2010).

- The Information Records Management team are also developing plans to roll out a training programme to ensure all staff are aware of CBCs Information Handling Policies.

Consideration should be give to providing a programme of training for Information Asset Owners and line managers to ensure relevant staff are appropriately trained in policy creation, management and monitoring, to ensure the Plan / Do / Check / Act continuous improvement model is successfully implemented..

Appendix A – Information Governance Framework Diagram

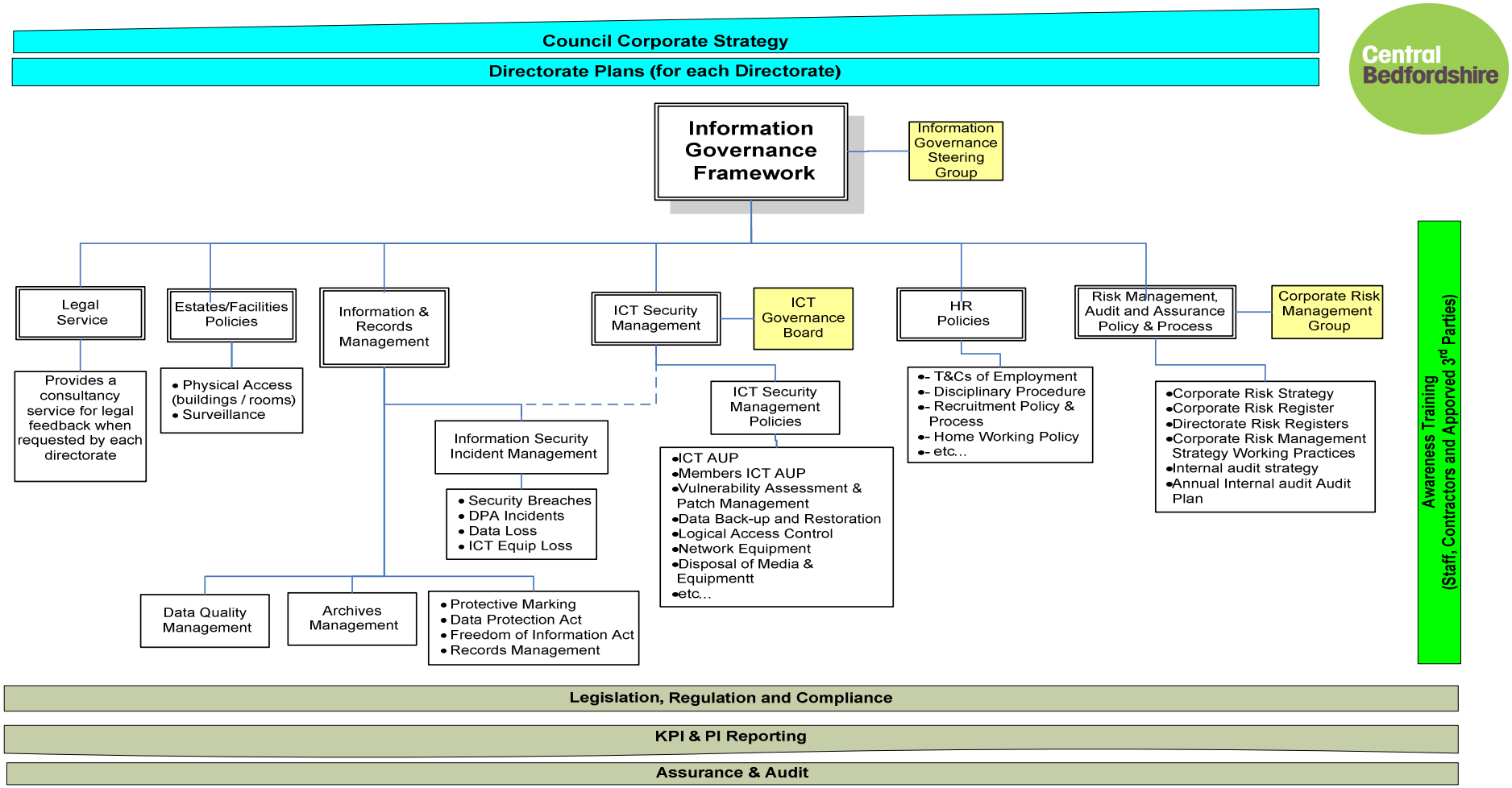

Figure 2 – Information Governance Framework

Appendix B – Detail Responsibilities of the IAOs

(Senior individuals involved in running the Council)

To ensure the governance of Central Bedfordshire Councils information all information assets must have an owner (an Information Asset Owner – IAO).

Members of staff at Head of Service level within the Council would typically be Information Asset Owners and the role can be described as:

- To understand and address risks to the information assets they and their team(s) 'own' and provide assurance to the SIRO on the security and use of these assets (understands the Council's plans to achieve and monitor the right Information Governance culture, across the Council and with its business partners and to take visible steps to support and participate in that plan (including completing own training)).
- Knows what information the Asset holds, and what enters and leaves it and why (maintains understanding of 'owned' assets and how they are used up to date; approves and minimises information transfers while achieving business purposes; approves arrangements so that information put onto portable or removable media like laptops, USB sticks and CD/DVD roms is minimised and are effectively protected to Information Governance standards; approves and oversees the disposal mechanisms for information of the asset when no longer needed).
- Knows who has access and why, and ensures their use is monitored and compliant with policy (understands the organisation's policy on access to and use of information; checks that access provided is the minimum necessary to satisfy business objectives; receives records of checks on use and assures self that effective checking is conducted regularly).
- Responsible for the authorisation of access to the assets, including the management of any authorised 3rd parties who are granted access to the information assets (or systems that they reside in).
- Understands and addresses risks to the asset, and provides assurance to the SIRO (conducts quarterly reviews of information risk in relation to 'owned' assets; makes the case where necessary for new investment or action to secure 'owned' assets; provides an annual written risk assessment to the SIRO for all assets 'owned' by them).
- Ensures the asset is fully used for the benefit of the organisation and its customers, including responding to requests for access from others (considers whether better use of the information is possible or where information is no longer required); receives, logs and controls requests from others for access; ensures decisions on access are taken in accordance with Information Governance standards of good practice and the policy of the organisation.

Appendix C – Information & Records Management

1. Information and Records Management Policy
2. Freedom of Information Policy
3. Data Protection Policy
4. Environmental Information Regulations Policy
5. Reuse of Public Sector Information Regulations Policy
6. Information Governance and Security Policy
7. How to use Information Guidelines
8. Service Level Agreement BBC005 for Archives and Records between Bedford Borough Council and Central Bedfordshire Council

Appendix D – Applicable Legislation

- Data Protection Act 1998
- Data Protection (Processing of sensitive personnel data) Order, 2000
- Computer Misuse Act 1990
- Copyright Designs and Patents Act, 1998 the Copyright (Computer Software) Amendment Act
- The Obscene Publications Act
- Regulation of Investigatory Powers Act (RIPA) 2000
- The Telecommunications Act (Lawful Business Practice Regulations 2000)
- Crime and Disorder Act, 1998
- Criminal Procedures And Investigations Act, 1996
- Health & Safety at Work Act 1974
- Freedom of Information Act 2000
- Children's Act 2004
- Environmental Information Regulations, 1992
- Human Rights Act 1998
- Limitations Act 1980
- Local Authorities (Access to Information) Act 1985
- Local Government Act 1972
- Re-use of Public Sector Information Regulations 2005
- Taxes Management Act 1970
- Common Law (The rights of citizens to have their information treated as confidential is enshrined in the law of the land. Individuals may be personally liable if they contravene this law).

Principal standards affecting CBC:

- GCSx CoCo (Government Connect Code of Connectivity)
- PCI-DSS (Payment Card Industry Data Security Standard)

- HMG Security Policy Framework (SPF)
- ISO/IEC 27001/2-2005 (Information Security)
- BS 15489-1:2001 (Information and Documentation. Records Management. General)
- ISO/IEC 25999 (Business Continuity)
- DETR/LGA guidance notes on 1972 s.224 'proper arrangements' 1999
- Lord Chancellor's Codes of Practice under ss.45-46 of the FOI Act , 2002

Appendix E – Performance Management & Data Quality

1. Performance Manual – containing the performance framework and the performance strategy, policy and action plan

Appendix F – Information Security Incident Management

1. Information Security Incident Management Process (update drafted, sign-off expected summer 2010)
2. ICT Service Desk Policy Procedures (expected summer 2010)
3. Data Protection Policy (Ref Appendix C)

Appendix G – ICT Service

ICT End-User Security Policies

1. ICT Acceptable Use Policy (AUP)
2. GCSx Acceptable Use Policy (AUP)
3. Members ICT Acceptable Use Policy (AUP)
4. Information Governance & Security Policy (Ref Appendix C)

ICT Security Management Policies/Standards and Processes

5. ICT Change Management Process
6. 3rd Party Remote Access Standard
7. Information Security Awareness Training
8. ICT Vulnerability Assessment & Patch Management
9. ICT Disposal of Media and Equipment
10. ICT Corporate Induction Security Awareness
11. ICT Security Incident Response (drafted, sign-off summer 2010)
12. ICT Data Backup & Restoration (drafted, sign-off summer 2010)
13. ICT Content Filtering & Malware Protection (drafted, sign-off summer 2010)
14. ICT Online Social Network (drafted, sign-off summer 2010)
15. ICT Workstation/Laptop configuration (drafted, sign-off summer 2010)
16. ICT Physical Security (drafted summer 2010)
17. ICT Penetration Testing (inc. IT Health Checks) (drafted, sign-off summer 2010)
18. ICT Logical Access Control (drafted, sign-off autumn 2010)
19. ICT Network Equipment Configuration (drafted, sign-off autumn 2010)
20. ICT Networks & Firewall Management (expected autumn 2010)
21. ICT Server Windows 2003/2008 Configuration (expected autumn 2010)
22. ICT Logging and Monitoring (expected autumn 2010)
23. ICT Cryptographic Key Management (expected autumn 2010)
24. ICT Software Acquisition and Acceptance Policy (expected winter 2010)
25. ICT Software Development Lifecycle (expected winter 2010)
26. Wireless Configuration (expected winter 2010)

Appendix H – Properties & Facilities

1. Procedures for issuing, updating and revoking swipe cards
2. Access to buildings request form
3. Policy for granting access to building (expected December 2010)
4. Policy for Surveillance systems (e.g. CCTV) (expected December 2010)

Appendix I – Human Resources Service

1. Terms & Conditions of Employment
2. Disciplinary Procedure
3. Recruitment Policy and Process
4. Leavers Process
5. Baseline Personnel Security Standard (BPSS) Recruitment Clearances Verification for GCSx Authorisation record
6. Home Working Policy

Appendix J – Risk Management, Audit & Assurance

1. Corporate Risk Management Strategy
2. Corporate Risk Management Policy Statement
3. Corporate Risk Management Strategy Working Practices 2009/10
4. Strategic Risk Register
5. Directorate Risk Registers
6. Service Risk Registers
7. Internal Audit Strategy
8. Internal Audit Charter
9. Strategic Internal Audit Plan
10. Annual Internal Audit Plan
11. Outcomes of internal and external audit reviews and other inspections
12. Corporate Health and Safety Policy Statement