Agenda Item: 10

Meeting: **Executive**

Date: **23 June 2009**

Subject: **Information Governance and Security Policy**

Report of: Portfolio Holder for Business Transformation.

Summary: This report seeks Executive approval for the Information Governance and Security Policy which is the final policy document in the Council's suite of information management policies to be presented to the Executive. This Policy incorporates the Statement of Application of Information Management Policies to Elected Members (at Annex A to the Policy).

Advising Officers:	Richard Ellis, Director of Business Transformation. Clive Heaphy, Director of Corporate Resources.
Contact Officers	Ian Porter, Assistant Director (Policy, Partnerships & Performance). Caroline Carruthers, Assistant Director (Property & ICT).
Public/Exempt:	Public
Wards Affected:	All
Function of:	Executive
Key Decision	Yes
Reason for urgency/ Exemption from call-in (if appropriate)	Not applicable.

RECOMMENDATIONS:

1. That the Executive:

(a) approves the Information Governance and Security Policy, attached at Appendix A, for implementation.

(b) delegates the responsibility for the insertion of changes requested by the Committee to the Assistant Director (Policy, Partnerships & Performance) in conjunction with the Assistant Director (Property & ICT).

(c) approves the Statement of Application of Information Management Policies to Elected Members, attached as Annex A to the Information Governance and Security Policy.

Reason for Recommendations	*Central Bedfordshire Council has a need to meet a number of national standards and legal requirements relating to information and its management. Compliance is ensured and evidenced through an approved suite of information management policies of which the Information Governance and Security Policy that is the subject of this report is one element. This policy is also a prerequisite of the Government Connect Code of Connectivity (CoCo).* *As there are aspects of this suite of information management policies from which elected members are exempt, these exemptions also need to be agreed and communicated.* *This report seeks Executive approval for the final policy in this suite, namely the Information Governance and Security Policy (Appendix A) as well as the Statement of Application of Information Management Policies to Elected Members (Annex A to the Policy).*

Background

1. Central Bedfordshire Council has a need to meet a number of national standards and legal requirements relating to information and its management. As information is a key corporate asset and central to everything the Council does, we need to know and have confidence:
   - about where it is and who is looking after it during the course of its lifecycle;
   - that it is available to those that need access to it; and
   - that its security is guaranteed and everyone in the Council knows how to handle sensitive information.

2. Having accurate, relevant and accessible information is vital to the efficient management of the Council. The Council must balance its aim to be open in providing information to the public and stakeholders with its obligations and duties around confidentiality and data protection for certain types of sensitive information. This balance, on which much confidence and trust is founded, requires the Council to:
   - create and manage all its records efficiently;
   - make them accessible when needed;
   - protect and store them securely; and
   - dispose of them safely at the appropriate time.

3. To ensure the Council has a robust framework for information management in place, we have been developing a suite of policies which set out arrangements for:

   - **ICT provision** in terms of the hardware and software all members and officers have access to and its acceptable use;
   - **access to information** - to ensure that the public have access to information through the appropriate legislative mechanisms;

- **information and records management** – to ensure the Council has the appropriate mechanisms in place to manage its records and information assets during the course of their lifecycles in accordance with relevant legislation and to support the Council's efficiency as an organisation; and
- **information assurance and security -** ensuring correct mechanisms are in place to minimise the adverse risk that can result from poor information governance and security.

4. Much of this information management framework has already been set out in the policies approved by the Shadow Executive between February and May 2009:

- Data Protection Policy (in response to Data Protection Act 1998) – approved 17 February 2009;
- Freedom of Information Policy (in response to Freedom of Information Act 2000) – approved 17 February 2009;
- Environmental Information Regulations Policy (in response to Environmental Information Regulations 2004) – approved 17 February 2009;
- Re-use of Public Sector Information Regulation Policy (in response to Re-use of Public Sector Information Regulations 2005) – approved 17 February 2009;
- ICT Acceptable Use Policy - approved 17 March 2009;
- Information and Records Management Policy – approved 17 March 2009; and
- Members' ICT Provision Policy from June 2009 onwards – approved 12 May 2009.

A final key component of information management is effective information governance and security, which is the subject of the policy document being considered at this Committee.

Information Governance and Security Policy

5. The Information Governance and Security Policy, attached at Appendix A, is intended to provide the Council with an effective governance and security management framework for the protection of the Council's information assets. It follows and addresses the widely accepted key principles of good information management and governance:

- **Confidentiality** – confining 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 and records are 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.

6. Given the diverse and complex nature of the Council's business, the policy also sets out the mandatory security requirements involved in meeting the current and emerging government/industry standards including the:

   (a) **Payment Card Industry Data Security Standard (PCI DSS)** which seeks to enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally in response to increasing credit and debit card security threats, and is designed to prevent credit card fraud, hacking, and other risks; and

   (b) **Government Connect Code of Connectivity (CoCo)** which is a pan-government programme providing an accredited and secure network between central government and every local authority in England and Wales. This requires all local authorities to have compliant security controls in place, no later than September 2009, before they can be connected to the GCSx (Government Connect Secure Extranet) which is part of the wider Government Secure Intranet (GSi) providing connectivity to nearly all central departments.

   Since April 2009, the Department for Work and Pensions (DWP) data access policy has required exchanges of sensitive personal data with local authorities to take place via Government Connect. The Council requires access to DWP systems and data to deliver Housing and Council Tax Benefits. Government Connect is also being used to exchange information for Youth Offending, Trading Standards, Registrars and Parking services and also offers a platform to be used for shared services.

   The approval of an Acceptable Use Policy and an Information Security Policy and security awareness training for all staff are all pre-requisites to achieving compliance.

7. This Information Governance and Security Policy will be reviewed annually or more frequently if a specific governance risk is identified or a new security threat arises.

Information Governance arrangements

8. The public sector in the UK has had a number of high profile information losses and breaches which have highlighted the need for all public sector organisations to have robust and enforceable security policies and 'fit for purpose' governance arrangements in place. These need to be kept under constant review as the rules and industry standards for information governance continue to be tightened.

9. At Central Bedfordshire Council, ultimate responsibility for information governance and security rests with the Chief Executive of the Council, with delegated authority to the Senior Information Risk Owner (SIRO), Director of Business Transformation.

10. To support the SIRO and ensure information management and governance become firmly embedded within both strategic and operational thinking and behaviour across the Council, an officer Information Governance Steering Group is being established. This Steering Group will be chaired by the SIRO and will have representation from all key service areas and its members will be responsible for cascading key messages to officers in their service areas.

11. The Information Governance Steering Group will report to the Central Bedfordshire Management Team on the delivery of information management and governance in Central Bedfordshire Council including arrangements for:

- ICT,
- Data Quality,
- Data Protection and Information Sharing,
- Information and Records Management,
- Freedom of Information and Confidentiality,
- developing and maintaining all information governance-related policies, standards, procedures and guidance,
- co-ordinating information governance in Central Bedfordshire Council, and
- raising awareness of information governance.

Information Governance and Elected Members

12. The Council's approved information management policies apply to all employees, employees and agents of external organisations who in any way support or access any Council information system, and all Elected Members of the Council unless a specific exemption is identified. These exemptions are set out in the Statement of Application of Information Management Policies to Elected Members which is attached for consideration and approval at Annex A to the Information Governance and Security Policy.

13. This Statement will be reviewed annually or more frequently as amendments or additions to the approved suite of information management policies are made.

Conclusion and Next Steps

12. Given the increasing volume and reliance on information and records, created and stored in both electronic and physical environments, any information governance and security arrangements must give effective support to those services and activities which rely on such information and embed a heightened sense of awareness of information management in the Council's culture.

14. Following approval of this policy document, the Council will have approved the full suite of information management policies. We will then need to ensure that everyone is aware of their individual responsibilities and that appropriate arrangements are put in place to embed these policies consistently across the organisation. The Information Governance Steering Group chaired by the Director of Business Transformation will oversee this and an early task will be to commission the delivery of an awareness and training programme.

15. As security awareness training is a prerequisite of the Government Connect Code of Connectivity (CoCo) compliance, this will need to be prioritised so that when our CoCo submission is made by the Section 151 Officer (Director of Corporate Resources) at the end of August 2009, this self assessment can indicate those actions which have been implemented (including the approval of the ICT Acceptable Use Policy and an Information Security Policy) and/or the plans that are in place for these (including staff training) to be embedded by the end September 2009.

CORPORATE IMPLICATIONS

Council Priorities:

Efficient and effective information governance and security arrangements are essential to the Council's performance and reputation. This report aims to ensure that the availability, integrity and confidentiality of the ICT and information management systems are maintained at a level which is appropriate for the Council's needs. These include the need to support the work of officers and councillors in meeting Central Bedfordshire Council's objectives and to be an open and trusted authority where appreciation of security and governance requirements is an intrinsic part of the organisation's culture.

The service transformation agenda is also critically dependent on effective information management and connectivity across local authorities and with government.

Financial:

The CBMT will consider the level of additional resources (both staffing and financial) required to sufficiently embed the suite of information management policies including an appropriate training and awareness programme.

Legal:

The Council must comply with all relevant UK and European legislation and standards, including principal **legislation**:

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

- Limitations Act, 1980.

and principal industry **standards:**

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

Risk Management:

The aim of this Information Governance and Security Policy is to:

- minimise the risk to public information by protecting it against unauthorised access and potential misuse; and
- put in place governance arrangements to ensure that our suite of approved policies are regularly reviewed to ensure that they are fit for purpose and adhere to appropriate legislative requirements.

Staffing (including Trades Unions):

See finance implications above.

Equalities/Human Rights:

The Council is required under equality legislation to collect and analyse a variety of information relating to service users and employees in order to ensure the promotion of equality of opportunity. Some of this information can be very confidential and the Council must ensure that such information is secure and used appropriately.

Sections of the information governance arrangements (email/internet usage) are directly concerned with the safeguarding of the Council's equalities and diversity policies.

Community Safety:

There are no community safety impacts directly associated with this report.

SustainabilityClimate Change:

There are no sustainability/climate change impacts directly associated with this report.

Appendices:

Appendix A – Central Bedfordshire Council's Information Governance and Security Policy

Background Papers (open to public inspection):

Location of papers: Priory House, Chicksands