CABINET
1 DECEMBER 2009

ITEM NO. .....

CORPORATE INFORMATION GOVERNANCE

Responsible Cabinet Member – Councillor Chris McEwan,
Efficiency and Resources Portfolio

Responsible Director – Paul Wildsmith, Director of Corporate Resources

SUMMARY REPORT

Purpose of the Report

1. The purpose of this report is to seek approval for the Corporate Information Governance Policy and Strategy, the Information Security Policy and associated delivery framework.

Summary

2. In April 2009 Cabinet approved an ICT Strategy that included in its delivery programme 'the implementation of robust and secure information management processes and systems'. Included in the delivery programme was the action to review the Council's Corporate Information Governance Policy approved by Cabinet in February 2008.

3. This review of the current Information Governance Policy and delivery framework has concluded and resulted in a proposed revised Corporate Information Governance Policy and Strategy, the development of an Information Security Policy, a refined delivery framework and the formulation of a high level work programme.

Recommendation

4. It is recommended that the:-

   (a) Corporate Information Governance Policy, Strategy and Information Security Policy at **Appendices A, B and C** be approved;

   (b) role and terms of reference of the Corporate Information Governance Group (CIGG) at **Appendix D** be approved; and

   (c) delivery work programme at **Appendix E** be noted.

Reasons

5. The recommendations are supported by the following reasons :-

   (a) A strategic risk based approach to information governance and information security management supported by demonstrable and visible senior management support will ensure that legal and regulatory requirements and best practice are embedded into business as usual activities and consistently applied across the Council.

   (b) The implementation of the policies and delivery of the work programme will provide the Council, its partners, key stakeholders, inspectorates and other interested parties with an appropriate level of assurance that information is managed in an efficient, effective and secure manner.

Paul Wildsmith
Director of Corporate Services

Background Papers

Cabinet Report 28 April 2009 – ICT Strategy
Cabinet Report 12 February 2008 – Corporate Information Governance Policy

Peter McCann: Extension 156494

S17 Crime and Disorder	There is no specific crime and disorder impact.
Health and Well Being	There is no specific health and well-being impact.
Sustainability	There is no specific sustainability impact.
Diversity	There is no specific diversity impact.
Wards Affected	All wards are affected equally.
Groups Affected	All groups are affected equally.
Budget and Policy Framework	This report does not recommend a change to the Council's budget or policy framework.
Key Decision	This is not a key decision.
Urgent Decision	For the purpose of the 'call-in' procedure this does not represent an urgent matter.
One Darlington: Perfectly Placed	This decision will not have a direct impact on the objectives of the Sustainable Community Strategy but will support elements of it.
Efficiency	The tasks contained within the associated Policy and Strategy delivery framework support the Council's ongoing efficiency programme.

MAIN REPORT

Background

6. In April 2009 Cabinet approved a refreshed ICT Strategy that identified as one of its key delivery programmes 'the implementation of robust and secure information management processes and systems' (min ref C199/Apr/2009). Within this delivery programme was the action to review the Corporate Information Governance Policy approved by Cabinet in February 2008 (min ref C175/Feb/2008) and develop and implement a new programme of work focusing on information security and data handling to complement and enhance the established information governance strategic policy framework.

7. In addition, responsibility for the provision of information governance related services, excluding the handling of information requests was transferred recently to Xentrall to increase resilience and improve efficiency.

8. This reports sets out the results of the comprehensive review of the Council's information governance policy and delivery framework. The objectives of the review were to ensure that:

   (a) information governance policies were fit for purpose, aligning information management strategies and activities with business objectives and priorities, and

   (b) a robust and sustainable information management and control environment was defined, implemented and embedded as part of a structured work programme

Corporate Information Governance Policy and Strategy

9. The Corporate Information Governance Policy approved in February 2008 was implemented through the cross-departmental Corporate Information Governance Group (CIGG) chaired by the Head of Corporate Assurance who reported progress six-monthly to the Audit Committee.

10. This Policy has been reviewed and on reflection was considered to include supporting information and development plans, which whilst constituting important information, was not appropriate for inclusion in the policy document. The policy document has therefore been revised and reformatted and is shown at Appendix A, with supporting information being included as appropriate in the Information Governance Strategy, the CIGG terms of reference, and the implementation work programme.

11. The Information Governance Strategy developed in support of the revised Policy is shown at Appendix B. This Strategy sets out the Council's approach in providing a robust and sustainable information governance framework for the management of information in line with the Corporate Information Governance Policy.

Information Security Policy

12. Information security management is concerned with the preservation of confidentiality, integrity and availability of information and the protection of information from a wide range of threats. The objective of information security management is to ensure service continuity, minimize business risk and maximise the opportunity to provide excellent services and support good decision making.

13. The review recognised the need for an Information Security Policy to complement and support the Information Governance Policy; an approach which is endorsed by Central Government which requires that all local authorities should be compliant with the ISO27002 Code of Practice for Information Security Management. The Information Security Policy shown at Appendix C is a high level policy statement which will be supported by a range of more detailed tactical and operational policies to be developed by CIGG. The implementation of these policies will significantly enhance the control and management of our information assets, and will also place the Council in a state of compliance with the Code of Practice.

Corporate Information Governance Group (CIGG)

14. The CIGG has a critical role in the development and implementation of information management related policies, procedures and working practices, and their terms of reference set out at Appendix D have been reviewed and revised to reflect this.

Work Programme

15. An implementation work programme has been developed comprising a summary of key tasks to be completed over the coming months and is set out at Appendix E. Detailed project plans will be developed for those tasks highlighted with CIGG being responsible for approving and monitoring the implementation of each plan.

Outcome of Consultation

16. The Policies and Strategies were devised with reference to recognised international quality standards and relevant professional organisations such as the Records Management Society.

APPENDIX A

Corporate Information Governance Policy

1. INTRODUCTION

The Council recognises the importance of reliable information to support the provision of good quality services. Information governance plays a key part in ensuring the reliability of this information.

Information Governance gives assurance to the Council, its customers and other stakeholders that all information, including confidential and personal information, is dealt with in accordance with legislation and regulations, and its confidentiality, integrity and availability is appropriately protected.

2. SCOPE

This policy covers

- all information processed by the Council,
- all information processed on behalf of the Council
- all information systems purchased, developed or managed by the Council
- all information systems purchased, developed or managed on behalf of the Council
- all employees and Members of the Council
- all contractors and sub-contractors of the Council as applicable

3. PRINCIPLES

For the purpose of this policy the following three principles have been identified

i. openness
ii. information security
iii. information quality assurance

i. Openness

The Council will ensure that

- there is an appropriate balance between openness and confidentiality in the management and use of information
- information is classified and where appropriate kept confidential, in line with the principles of Caldicott and the requirements of the Data Protection Act 1998.
- non-confidential information is available to the public in accordance with the requirements of the Freedom of Information Act 2000
- the Council regards all identifiable personal information relating to staff as confidential except where legislation requires otherwise
- there are clear procedures and arrangements for handling requests for information
- there are clear procedures and arrangements for liaison with the press and other media
- integrity of information is monitored and maintained
- information is managed in accordance with the Council's records management policies and retention schedules
- information is protected via appropriate computer system resilience and business continuity procedures

- there are clear procedures for the reporting and management of breaches of confidentiality
- awareness and understanding of all staff and Members with regard to their responsibilities is assessed and appropriate training provided.
- risk assessments are regularly undertaken to ensure that effective and appropriate information governance controls are in place

ii. Information security

The Council will ensure that

- policies for the effective and secure management of its information assets and resources are implemented in accordance with the requirements of the BS ISO/IEC 27000 series of information security management, and other related standards

iii. Information quality assurance

The Council will ensure that

- policies for the effective management of records are implemented in accordance with the BS ISO/IEC 15489-1:2001 Records Management standard
- policies for the effective management of data quality are implemented in accordance with best practice

4. CONTINUOUS IMPROVEMENT

The Council will ensure that

- appropriate monitoring procedures are in place to assess the effectiveness of policy implementation
- where weaknesses are identified appropriate remedial action is taken in a timely and effective manner
- monitoring and review procedures and associated remedial actions are based upon regular risk assessments

5. INFORMATION GOVERNANCE MANAGEMENT

The Council will ensure that information governance is managed as part of an Information Security Management System (ISMS) as defined in BS ISO/IEC 27001:2005.

6. REVIEW

This policy will be reviewed at least annually by the Corporate Information Governance Group (CIGG).

APPENDIX B

Information Governance Strategy

1. *INTRODUCTION*

The Council recognises the importance of reliable information to support the provision of good quality services. Information governance plays a key part in ensuring the reliability of this information.

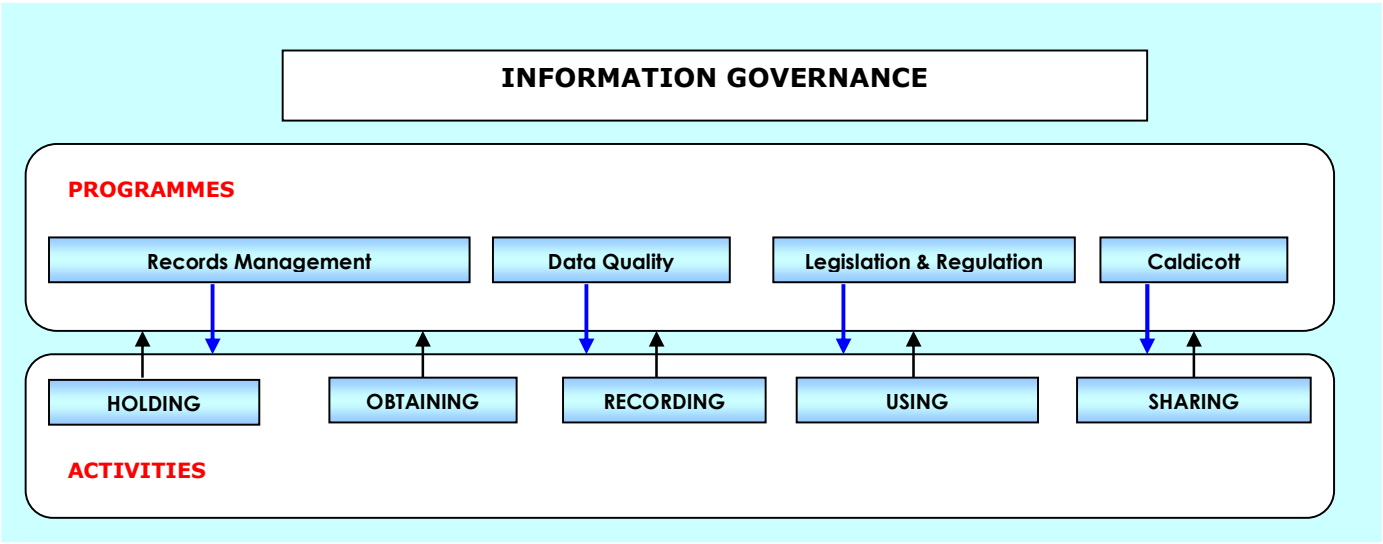
Information Governance (IG) gives assurance to the Council, its customers and other stakeholders that all information, including confidential and personal information, is dealt with in accordance with legislation and regulations, and its confidentiality, integrity and availability is appropriately protected.

2. *PURPOSE*

This strategy sets out the Council's approach in providing a robust, sustainable IG framework for the management of information in line with the Information Governance Policy. This strategy can not be properly implemented in isolation as there are integral links with IG across all aspects of the Council's business activities such as service planning, performance management, and strategic risk management.

3. *SCOPE*

The scope of the strategy is shown in the diagram below.



The Council will develop formal projects in accordance with the Corporate Project Management methodology for the delivery of the programmes identified above. Progress on the delivery of the projects will be monitored by the Corporate Information Governance Group (CIGG).

4. *REVIEW*

The delivery of this strategy will be regularly reviewed in line with the Council's corporate project management methodology and reporting responsibilities as outlined in the CIGG terms of reference.

APPENDIX C

Information Security Policy and Objectives

Table of Contents

1. Statement of Management Intent

Darlington Borough Council recognises the importance of accurate information and the need for that information to be readily available to those who need it, and protected from unauthorised access by those who do not. The increasing value and criticality of information together with the need to share it present increased information security risks.

The Council takes the management of risks associated with information security very seriously, and proper controls need to be established and implemented to protect against the constantly evolving list of information security risks.

It is necessary for all Council employees to support this process and adhere strictly to information security policies and guidelines, thereby ensuring an appropriate level of security of information assets under the Service's control or stewardship.

2. Policy

The purpose of the policy is to appropriately protect the Council's information assets from threats, whether internal or external, deliberate or accidental.

The Chief Executive has approved this policy.

It is the policy of Darlington Borough Council to ensure that:

- a framework for setting measurable information security objectives is established
- risks are identified and managed in line with approved strategic risk management procedures
- criteria for accepting risks and identifying the acceptable level of risk are established
- information is protected against unauthorized access
- confidentiality of information is assured
- integrity of information is maintained
- regulatory and legislative requirements are met
- business continuity plans are produced, maintained and tested
- information security training is available to all staff
- all breaches of information security are reported to and investigated by the Information Security Manager

Procedures exist to support this policy.

Business requirements for the availability of information and information systems will be met.

The Head of Corporate Assurance has direct responsibility for maintaining the policy and providing advice and guidance on its implementation.

All managers are directly responsible for implementing the policy within their business areas, and for adherence by their staff.

It is the responsibility of each member of staff to adhere to the policy.

3. Objectives

The objective of information security is to protect the interests of all stakeholders relying on the information and processes, systems and communications services supplied by, managed by or under the control of the Council that handle, store and deliver information, from harm resulting from failures of confidentiality, integrity and availability.

Security objectives are met when

- information is available and usable when required, and the systems that provide it can appropriately resist attacks and failures
- information is observed by or disclosed to only those who have the right to know
- information is protected against unauthorised modification
- business transactions, as well as information exchanges between organisation locations, or with partners and stakeholders, can be trusted
- information security requirements of customer charters are fulfilled
- all third party suppliers perform to minimum information security related standards

4. Review

This policy will be reviewed annually by the Corporate Information Governance Group.

APPENDIX D

CORPORATE INFORMATION GOVERNANCE GROUP (CIGG)

Terms of reference

The Corporate Information Governance Group is accountable to the ICT Strategy Group for reporting purposes as they are responsible for "robust and secure information management" as set out in section 3 of the ICT Strategy 2009 – 2012 document.

Function and responsibilities

Information Governance is about managing information and access to it, from the time it is created to the point of disposal, in a way that is efficient, secure, responsive to business needs, and compliant with the law.

The CIGG will

1. provide strategic direction regarding information management

2. ensure information governance becomes embedded into the actions of all management and stakeholders

3. ensure consistency in the way information is held, obtained, recorded, used, and shared

4. develop and approve (where appropriate) tactical and operational information management policies

5. assess the quality of information and the tools, policies, procedures and systems used in the delivery of services

6. provide a framework for information governance bringing together all codes of practice, standards, and best practice relating to information governance and information security management

7. consult and liaise with other groups of the Council, its partners and stakeholders dealing with aspects of the information governance agenda

Reporting arrangements

The CIGG will report to six-monthly to the ICT Strategy Group on progress and planned developments. In turn the ICT Strategy Group is required to report six-monthly to the Audit Committee on progress in implementation of the ICT Strategy.

APPENDIX E

CORPORATE INFORMATION GOVERNANCE GROUP WORK PROGRAMME 2010

Task	Project	Target date
INFORMATION SECURITY		
Develop tactical and operational information security policies	No	January 2010
Employees guide to Information Security	Yes	March 2010
Develop information security training and awareness programme	Yes	March 2010
Develop and implement corporate information security management system	Yes	June 2010
INFORMATION GOVERNANCE		
Records management programme	Yes	December 2010
Data quality self assessment programme	Yes	September 2010
Information legislation and regulation review (including Caldicott)	Yes	June 2010
Information Assurance self assessment programme	Yes	March 2010
Develop and designate key service based roles and responsibilities	No	June 2010