Derby City Council

Information Governance Strategy

V1.0

Information Governance Framework
IGF/IGML3

Document owner	Roger Kershaw, Strategic Director Resources
Document author	Richard Boneham, Head of Governance & Assurance
Approved by and when	Information Governance Board 19 June 2013
Date of document	February 2013
Version	1.0
Document classification	Internal
Document distribution	Internal
Document retention period	Until date of next review
Location	iDerby
Review date of document	August 2014

If you require this document in large print, on audio tape, computer disc or in Braille please contact the document manager.

Date Issued	Version	Status	Reason for change
February 2013	0.1	Draft	New strategy document
June 2013	0.2	Draft	Revision
June 2013	1.0	Issued	

To make sure you are using the current version of this policy please check on iDerby under **Governance/Information Governance** or contact the Information Governance Manager when using printed copies

CONTENTS

1. INTRODUCTION

Information is a vital asset in terms of the efficient management of services and resources throughout the Council. It plays a key part in governance, service planning and performance management.

It is therefore of paramount importance that information is efficiently managed, and that appropriate policies, procedures and management accountability and structures provide a robust governance framework for information management to assure and demonstrate the proactive use of information as determined by legislative acts, statutes, regulatory requirements and best practice.

Information Governance is a framework for handling information in a confidential and secure manner to appropriate ethical and quality standards. It brings together within a singular cohesive framework, the interdependent requirements and standards of practice. It combines Information Security, Corporate Governance and Business Continuity, and the increasing legislative and regulatory requirements, into a single unified management framework.

Information Governance is not simply a matter of good corporate housekeeping. Good Information Governance can undoubtedly lead to efficiency gains and make for more effective management.

2. PURPOSE

This purpose of this strategy is to fulfil the objectives of the Information Governance Policy, including ensuring business efficiency, effective service delivery, and compliance with the individual and social obligations the council has in respect of all the information it holds. Information Assurance and Information Risk Management (IRM) are the means by which this will be done.

The Council recognises the importance of reliable information to support the provision of good quality services. Information governance and assurance play a key part in making sure of the reliability of this information as service delivery relies on the right information being available to the right people at the right time, whilst maintaining confidentiality.

This Information Governance Strategy provides a mechanism for making sure that the Council meets its responsibilities in the following areas:

- The growing need for partnership sharing of information means that it must apply the common standards mandated by the Code of Connection and Connecting for Health.
- The LGA - Local Government Association's 'Data Handling Guidelines' apply the government's Security Policy Framework to local authorities and sets out standards to be applied by the Council to make sure of security of data, and be seen to do so
- The mandatory Records Management Code of Practice

However, in addition to these standards there is a body of best practice measures, which if applied will assist the Council in discharging its obligations to enact effective IRM.

This strategy sets out the approach to be taken within the Council to make sure of legal and regulatory compliance for the management of information.

The Information Governance Strategy cannot be seen in isolation as information plays a key part in Corporate Governance, strategic risk, service planning, performance and business management. This Strategy, therefore, is closely linked with other strategies to make sure of integration with all aspects of the Council's activities.

3. SCOPE

The principles cover all aspects of information handling within the Council including service user information, employee related information etc. The principles cover all aspects of handling information, including structured record systems (paper & electronic).

There are two key components underpinning this Strategy, which are:

- The Council's Information Governance Policy, which outlines the objectives for Information Governance
- The action / improvement plan arising from the ICO audit and our assessment against the NHS (Connecting for Health) Information Governance Toolkit standards,- Local authority version within the following initiative areas:
    - Information Governance Management
    - Confidentiality & Data Protection Assurance
    - Information Security Assurance
    - Secondary Use Assurance
    - Corporate Information Assurance

The Information Governance framework includes adherence to the following statutory legislation and standards:

- Data Protection Act (1998)
- Freedom of Information Act (2000)
- Records Management
- Information Security
- Information sharing
- Information Quality
- Confidentiality
- Openness/Transparency
- Legal Compliance

4. DEFINITIONS

Data Controller:
The person or organisation that collects personal data and decides on how to use, store or distribute that data

Data Processor:
Any person or organisation (other than an employee of the data controller) that processes the data on behalf of the data controller

Data Subject:
An individual who is the subject of the personal data

Personal Data:
Data that relates to a living individual that can identify the individual from this data or other information in the possession of the data controller

Sensitive Personal Data:
Data that relates to a living individual that includes racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, physical or mental health condition, sex life, criminal proceedings or convictions

5. ROLES AND RESPONSIBILITIES

5.1. Chief Executive

The Chief Executive takes overall responsibility for the Council's information governance performance and in particular is required to make sure that:

- decision-making is in line with Council policy and procedures for information governance and any statutory provisions set out in legislation
- that information risks are assessed and mitigated to an acceptable level.
- information governance performance is continually reviewed
- suitable action plans for improving information governance are developed and implemented

To satisfy the above responsibilities, the Chief Executive will nominate a Senior Information Risk Owner who will be accountable for the Council's overall information governance arrangements

5.2. Senior Information Risk Owner (SIRO)

The Chief Executive/Council must appoint a manager of an appropriate seniority as its SIRO. The Strategic Director of Resources is a member of the Chief Officer Group - COG and reports to the Audit & Accounts Committee on information governance matters, and is therefore an appropriate SIRO.

Responsibilities of the SIRO include:

- owning the information risk policy and risk assessment,
- acting as an advocate for information governance and assurance at COG and in internal discussions,
- chairing the Information Governance Board
- providing written advice to the Audit and Accounts Committee relating to information risk;
- managing information governance and assurance

5.3. Caldicott Guardian

The Caldicott Guardian is the senior role responsible for ensuring the Caldicott principles are met. The Caldicott Guardian acts as a conscience in matters of data confidentiality and sharing. They work as part of a broader Information Governance function within the Council. The role is specifically targeted towards Social Care/Health information and records. The key responsibilities of the Caldicott Guardian are:

1. **Strategy and Governance:**
   To act as a champion for data confidentiality at Directorate Management level and as part of the Council's Information Governance Board
2. **To provide confidentiality and data protection expertise:**
   To develop a knowledge of confidentiality and data protection matters including links with external sources of advice and guidance
3. **Internal Information Processing:**
   To ensure that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff
4. **Information Sharing:**
   To oversee all arrangements, protocols and procedures where confidential social or healthcare information may be shared with external bodies including disclosures to other public sector agencies and other outside interests

There are 6 principles relating to data handling and use that were established on which the role of Caldicott Guardian was based:

Principle 1 - Justify the purpose(s) for using confidential information
Principle 2 - Only use it when absolutely necessary
Principle 3 - Use the minimum that is required
Principle 4 - Access should be on a strict need-to-know basis
Principle 5 - Everybody must understand his or her responsibilities
Principle 6 - Understand and comply with the law

5.4. The Information Governance Board

Information Governance requires clear lines of accountability for policy, practice and implementation. The Information Governance Board, in conjunction with the Information Governance Manager, will make sure of coherence, clarity and consistency in the way information is governed within the Council.

The Information Governance Board is accountable to the Governance Board and the Audit and Accounts Committee. The Board has overall responsibility for overseeing the implementation of the Information Governance Framework, this Strategy, the Information Governance Policy and the Information Governance Action Plan. All are subject to periodic review and progress reported to the Governance Board and Audit and Accounts Committee. There is corporate representation on the Board to make sure that Information Governance is embedded within the organisational structure.

Information Governance Board has the following roles and responsibilities:

- Approval of corporate policies and procedures which make sure of:
  - compliance with legislation
  - data quality
  - information security (compliance with ISO 27001)
  - records management (compliance with ISO 15489)
- Co-ordination and approval of corporate standards for the mitigation of risk
- Monitoring compliance with the Information Governance Framework
- Establishing a policy for reporting, managing and recovering from information risk incidents, including losses of protected personal data and ICT incidents, defining responsibilities and making employees aware of the policy and reporting to Councillors if appropriate.

5.5. Information Governance Manager

The Information Governance Manager is responsible for:

- Co-ordinating all Information Governance initiatives and overseeing the production of the annual improvement plan / work programme
- the first point of contact on information governance matters for all officers and elected members, members of the public and the Information Commissioner.
- Providing operational support including training, query resolution, incident support and legal compliance requirements, e.g. Data Protection Act (1998) and Freedom of Information Act (2000) compliance
- Being the lead officer for the Information Governance Board
- Routine performance reporting to the Information Governance Board and Audit and Accounts Committee

The IGM reports to the Head of Governance and Assurance and plays a key role in supporting the development and communication of information governance policy, strategy and action plans and for making sure that the Council adopts information governance best practice and standards.

5.6. Strategic Directors

Each Strategic Director is responsible for the information within their Directorate and must therefore take overall responsibility for information governance matters. In particular Strategic Directors are required to:

- make sure that adequate resources are available to successfully manage information governance within their directorate
- assign a senior manager as the Directorate's Information Governance Champion to sit on the Information Governance Board
- support the implementation of corporate information governance associated policies and procedures
- identify their information assets (in all formats)
- categorise these information assets in a way that is meaningful to the directorate and identify for each information asset an 'Information Asset Owner'

Each Directorate is also responsible for:

- managing its own information risks,
- proper management of information risks,
- meeting the mandatory corporate information governance requirements and
- meeting the requirements of the Information Governance policy/strategy.

Directorates must have and execute plans to lead and foster a culture that values, protects, uses information for service delivery, and monitors progress when conducting a service user (including employees) survey or equivalent. Directorates must also reflect performance in managing information risk into HR processes in particular making clear that failure to apply directorate and corporate procedure is a serious matter, and in some situations non-compliance may amount to gross misconduct.

5.7. Information Asset Owners

Information Asset Owners (IAOs) must be senior officers involved in running the relevant business area. Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has accessed it and why. All information should be categorised in accordance with the Protective Marking Scheme and stored in line with the Council's eDRMS arrangements. This will facilitate an understanding of the risks to the information and how those risks need to be managed to make sure of compliance with legislation.

IAOs have the most work to do since they will be applying all the information governance related policies (see App B) to their services and all the information they use. They must identify and maintain a record of those employees, contractors and others with access to or involved in handling individual records containing personal data. IAOs must:

- make sure that information is used correctly and protected
- produce an Information Asset Register for their area of responsibility
- to make sure that security marking, legal admissibility and access controls are all properly applied.
- consider whether and how better use could be made of their information assets and to information held by other services.

5.8. Internal Audit

Internal Audit can provide assurance to the Council that it's Information Governance and Assurance Framework is operating according to its structure of policies, strategies and action plans.

5.9. Information Governance Team

The Information Governance team supports the Information Governance Manager by contributing to the development of information governance policy and strategy. The Team will also be the central co-ordination point for all responses to requests for information made under the Data Protection, Freedom of Information and Environmental Information legislation. The team maintains a record of all such information requests received and responded to and make sure that statutory deadlines are met.

5.10. Audit & Accounts Committee

The SIRO will report to Audit & Accounts Committee at least twice a year on information governance matters. The SIRO will highlight changes in framework and policy and detail the progress made in embedding the framework across the Council. The results of any compliance testing will also be reported where applicable.

5.11. Managers

Managers have a responsibility to make sure that all their employees are aware of the Information Governance Strategy and associated policies.

5.12. Employees

All employees are responsible for maintaining compliance with relevant legislation and the Council's Information Governance requirements.

6. PROCESS

6.1 Aims

Information Governance has four fundamental aims:

- To support the provision of high quality services by promoting the effective and appropriate use of information
- To encourage responsible employees to work closely together, preventing duplication of effort and enabling efficient use of resources
- To develop support arrangements and provide employees with appropriate tools and support to help them to carry out their responsibilities to consistently high standards
- To help organisations to understand their own performance and manage improvement in a systematic and effective manner

The aim of this Strategy is to make sure of the effective management of Information Governance by:

- Complying with all relevant legislation
- Establishing, implementing and maintaining policies for the effective management of information
- Making sure there is a consistent approach within the Council with regard to information management
- Recognising the need for an appropriate balance between openness and confidentiality in the management and use of information
- Making sure that all Council employees follow and promote best practice
- Developing an Information Governance culture throughout the Council
- Helping employees to manage personal information they are responsible for
- Reducing duplication and looking at new ways of working effectively and efficiently
- Minimising the risk of breaches of personal data
- Minimising inappropriate uses of personal data

6.2 Other key Information Governance metrics

- Information Governance assessment
- Serious Incident reporting and progressive comparison (biannual reporting to the Governance Board)

6.3 Information Governance Management Framework

Robust Information Governance requires clear and effective management accountability structures, governance processes, documented policies and procedures, trained employees and adequate resources. (See Appendix B for details).

The Electronic Document Records Management System (EDRMS) Project will have a significant positive impact on many areas of the Council's operations as it will help improved management of, and access to, the documents and records held within the organisation, as well as providing a secure, single data repository. The Information Governance Manager will work with the EDRMS Project Manager.

Information Security considerations include:

- development and management of the Council's information security policy
- investigation of technical security incidents and breaches
- periodic verification of compliance with policies via information security reviews
- provision of awareness and compliance programmes for the Authority

The Council will put in place appropriate policies and procedures to secure the quality of data it records and uses. The approach will ensure:

- a formal data quality policy and associated operational procedures and guidance for employees are in place, covering data collection, recording, analysis and reporting
- all data quality policies and procedures meet the requirements of any relevant national standards, rules, definitions and guidance, and define local practices and monitoring arrangements
- periodic review of all data quality policies and procedures
- data quality policies and procedures are appropriately accessible to employees
- consistent application of data quality policies, procedures and guidance

6.4 Conclusion

The implementation of Information Governance strategy, policy and action plan will make sure that information is legally, effectively and efficiently managed within the Council.

7. TRAINING REQUIREMENTS

All new employees will receive corporate induction training which includes all aspects of Information Governance including Data Protection, Information Security and Freedom of Information via the Council's corporate E-learning tool.
The Information Governance Manager is responsible for the delivery of all other Information Governance training and awareness sessions throughout the Council.

Subsequent training needs will be identified through the appraisal process / individual performance review process.

8. REFERENCES AND ASSOCIATED DOCUMENTATION

The Data Protection Act 1998

http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_1

The Freedom of Information Act 2000
http://www.opsi.gov.uk/Acts/acts2000/ukpga_20000036_en_1

The Human Rights Act 1998
http://www.opsi.gov.uk/ACTS/acts1998/ukpga_19980042_en_1

9. MONITORING COMPLIANCE WITH, AND THE EFFECTIVENESS OF, PROCEDURAL DOCUMENTS

Compliance with this Strategy will be monitored through its associated policies and the metrics identified in section 6.2.

These will help the effectiveness of the Strategy to be evaluated and a report presented to the Governance Board.

10. APPENDICES

Appendix A: Overview of legislation

Human Rights Act 1998
This Act became law on 2 October 2000. It binds public authorities to respect and protect an individual's human rights. This will include an individual's right to privacy (under Article 8) and a service user's right to expect confidentiality of their information at all times.

Article 8 of the Act provides that 'everyone has the right to respect for his private and family life, his home and his correspondence'. However, this article also states 'there shall be no interference by a public authority with the exercise of this right except as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, or the economic well-being of the country, for the prevention or detection of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others'.

Each organisation must act in a way consistent with these requirements. It must take an individual's rights into account when sharing personal information about them.

Freedom of Information Act 2000
This Act came into force on 1 January 2005. This act gives individuals right of access to corporate information held by the Council such as policies, reports, minutes of meetings.

Regulation of Investigatory Powers Act 2000
This Act combines rules relating to access to protected electronic information as well as revising the 'Interception of Communications Act 1985'. The Act aims to modernise the legal regulation of interception of communications in the light of the Human Rights laws and rapidly changing technology.

Crime and Disorder Act 1998
This Act introduces measures to reduce crime and disorder, including the introduction of local crime partnerships around local authority boundaries to formulate and implement strategies for reducing crime and disorder in that local area.

The Act allows disclosure of person identifiable information to the Police, Local Authorities, Probation Service or the Health Service but only if the purposes are defined within the Crime and Disorder Act. The Act does not impose a legal requirement to disclose/exchange person identifiable information and responsibility for disclosure rests with the organisation holding the information. There should be a Crime and Disorder Protocol governing the disclosure/exchange and use of personal information within a local authority boundary agreed and signed by all involved agencies and organisations.

The Computer Misuse Act 1990
This Act makes it a criminal offence to access any part of a computer system, programs and/or data that a user is not entitled to access. Each organisation will issue individual users an individual user ID and password which will only be known by the individual they relate to and must not be divulged / misused by other staff. This is to protect the employee from the likelihood of their inadvertently contravening this Act.

Each organisation will adhere to the requirements of the Computer Misuse Act 1990 by ensuring staff are made aware of their responsibilities regarding the misuse of computers for personal gain or other fraudulent activities. Any member of staff found to have contravened this Act will be considered to have committed a disciplinary offence and be dealt with accordingly.

The Justice and Coroners Act
This Act has amended the Data Protection Act to strengthen the Information Commissioner's inspection powers.

Appendix B:

Senior Roles		
Role	Filled By	Details
Accountable Officer	Chief Executive	Overall responsibility for all aspects of the Council's Information Governance
Information Governance Lead	Information Governance Manager	Responsibility for assessing, monitoring and reporting compliance with, and emerging issues in, Information Governance
Senior Information Risk Owner (SIRO)	Strategic Director - Resources	Implement and lead the Information Governance risk assessment and management process
Caldicott Guardian	Strategic Director – Adults, Health & Housing	Responsibility for safeguarding the confidentiality of, and access to, service user information
Information Security Officer	Information Governance Manager	Responsibility for ensuring compliance with Information Security Standards (ISO/IEC 27001:2005)
Information Governance Incident Management	Head of Governance & Assurance, Senior Information Risk Owner, Information Governance Manager	Responsibility for the incident management process / chairing incident panels / investigations and investigation subject matter expertise
Data Protection and Freedom of Information Lead	Information Governance Manager	Responsibility for assessing and monitoring compliance with Data Protection and Freedom of Information legislative requirements
Information Quality Lead	TBC	Best practice adopted by the NHS Information Governance Toolkit recommends that, an appropriate manager is identified or nominated to lead on the reporting of compliance against Information Quality requirements
Records Management Lead	Head of Governance and Assurance	Advice on, and monitoring compliance with, legal and best practice in records management

Key Policies		
Policy Name	Responsible Manager	Detail of Approving Body
Codes of Conduct		Council
Data Protection Act Policy	Information Governance Manager	Information Governance Board
Data Quality Policy and Procedures	Head of Performance & Improvement	Information Governance Board

Key Policies		
Policy Name	Responsible Manager	Detail of Approving Body
Network, Email & Internet User Policy	Information Governance Manager	Information Governance Board
Freedom of Information Act Policy	Information Governance Manager	Information Governance Board
Information Security Policy	Information Governance Manager	Information Governance Board
Records Management Strategy	Head of Governance & Assurance	Information Governance Board
Information Governance Policy	Head of Governance & Assurance	Audit and Accounts Committee
Information Governance Strategy	Head of Governance & Assurance	Audit and Accounts Committee
Remote Working Policy	Information Governance Manager	Information Governance Board
Records Retention and Disposal Policy	Information Governance Manager	Information Governance Board
Serious Untoward Incidents Policy	Director of Transformation,	

Key Governance Bodies		
Group / Committee	Accountability	Responsibility
Information Governance Board	To the Governance Board	Promote effective Information Governance, maintain a framework to ensure legal compliance, promote local-level responsibility and accountability
Governance Board	Audit & Accounts Committee	

Resources		
Area	Roles	Resource Access

Work Programmes		
Aspects	Lead(s)	Requirement

Training and Guidance		
Training Type	Details	Frequency
Data Protection Act	e-Learning	Every 3 years
Information Security	Part of induction e-learning	Refresh every 3 years

Incident Management		
Incident Type	Staff	Role

L1 **Information Governance Framework**

L2 **Information Governance Management**

L3 IG Strategy document
Governance Board TOR
Information Asset Register
Information Governance Strategy
Serious incident Policy

L2 **Confidentiality & Data Protection Assurance**

L3 Principles & Obligations
Data Protection Act Policy
L4 Data Protection operational guidance
Accessing & Storing Data
Records Retention schedule
Records management policy/strategy
Protective marking scheme/Classification
DPA/Caldicott Guidance
Confidential waste disposal
Business Impact Levels
Register of Information Sharing Agreements
Privacy impact assessments new systems

L2 **Information Security Assurance**

L3 Information security policy
Password policy
Network, Email & Internet User policy/electronic mail
Mail handling procedures
Monitoring policy
IT Security
L4 Anti-Virus Policy
Desktop and Laptop computer security policy
Starters & Leavers
Rules
Home & remote working policy
BYOD
Mobile computing
Code of Connect compliance documentation
User access management policies

L2 **Action Plan**