Derby City Council

Appendix 4

Information Risk Policy

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	
Date of document	December 2013
Version	1.0
Document classification	Internal
Document distribution	Internal
Document retention period	Until date of next review
Location	TBA
Review date of document	December 2016

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
June 2013	0.1	Draft	New Policy document
November 2013	1.0	Final	Approved by IGB

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

Equality impact assessment record	
Date of assessment	
Summary of actions from EIA	

Contents

Introduction and purpose

This Policy forms part of the Council's Information Governance Framework and sits at Level 3 under Information Governance Management. See Appendix 1.

This Policy establishes the Council's expectations and rules in respect of the effective protection of information through the management of the risks associated with it.

Scope

This Policy applies to all Council employees, including Councillors, consultants and temporary contractors who have authorised access to Council IT systems who work with and produce official records on behalf of the Council.

This policy relates to

Related Council strategies, policies, and procedures

- Information Security Policy
- Data Protection Act Policy
- Caldicott Principles
- Protective Marking Scheme
- Document Retention Schedule
- Desktop and Laptop Computer Security Policy
- Serious Incident Reporting Policy

Legislation, guidance and standards

The Council is required by law to comply with all relevant legislation or statutory guidance. All employees including temporary employees and agency staff, Elected Members, partners and external contractors must comply with the relevant legislation when acting on behalf of the Council.

The Council will comply with the following legislation and guidance, and any other legislation as appropriate:

- Data Protection Act 1998
- The Freedom of Information Act 2000
- Public Records Act 1958
- Re-use of Public Sector Information Regulations 2005
- Employment legislation
- Health and safety legislation

If you are not sure of your responsibilities under any of these laws, contact the Council's Information Governance Manager for further information.

Policy statement

The Council has approved the introduction and embedding of information risk management into the key controls and approval processes of all major business processes and functions of the Council. This decision reflects the high level of importance placed upon minimising information risk and safeguarding the interests of the citizens of Derby, our Members, our staff and the Council itself.

Information risk is inherent in all administrative and business activities and everyone working for or on behalf of the Council continuously manages information risk. The Council recognises that the aim of information risk management is not to eliminate risk, but rather to provide the structural means to identify, prioritise and manage the risks involved in all Council activities. It requires a balance between the cost of managing and treating information risks with the anticipated benefits that will be derived.

The Council acknowledges that information risk management is an essential element of broader information governance and is an integral part of good management practice. The intent is to embed information risk management in a very practical way into business processes and functions.

This document should be read in conjunction with the Information Security Policy.

Definitions

- **Risk**
  The chance of something happening, which will have an impact upon objectives. It is measured in terms of *impact* (*consequence)* and *likelihood*.
- **Consequence**
  The outcome of an event or situation, expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain. There may be a range of possible outcomes associated with an event.
- **Likelihood**
  A qualitative description or synonym for probability or frequency.
- **Risk Assessment**
  The overall process of risk analysis and risk evaluation.
- **Risk Management**
  The culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects.
- **Risk Treatment**
  Selection and implementation of appropriate options for dealing with risk. Conceptually, treatment options will involve one or a combination of the following five strategies:
    - Avoid the risk
    - Reduce the likelihood of occurrence

- Reduce the consequences of occurrence
- Transfer the risk
- Retain/accept the risk

- **Risk Management Process**
  The systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risk.

- **Information Asset**
  An information asset is a generic term to cover all information, or information system used by the Council. Information can take many forms and includes, but is not limited to, the following:

  - Hard copy data printed or written on paper or other medium
  - Data stored electronically
  - Communications sent by post/courier or using electronic means
  - Stored tape, video or other media
  - speech

- **Information risk management**
  The process of identifying vulnerabilities and threats to the information resources used by an organisation in achieving business objectives, and deciding what mitigating measures, if any, to take based on the value of the information resource to the organisation and the potential penalties for a failure to protect those resources.

- **An information security incident**
  An incident is any violation of the DCC Information Security Policy. Such an incident could compromise the confidentiality, integrity or availability of information or information assets, having and adverse effect on security, reputation, performance or ability to meet regulatory or legal obligations. It may fall into a broad range of events and includes, but is not limited to, incidents that effect disclosure, denial of access to, destruction or modification of the Council's data. Examples include;

  - The use of another user's login id
  - The unauthorised disclosure of information
  - Leaving confidential / sensitive files where they are accessible to non-authorised individuals
  - The loss of IT equipment whether accidental or through theft
  - Accessing a persons' record inappropriately, (to include viewing you own record, family member, neighbour, friend etc.)
  - Use of personal information for criminal/fraudulent intent e.g. ID theft

  Further details can be found in Appendix 1 of the Information Security Policy.

Roles and responsibilities

The Council Senior Information Risk Owner (SIRO) is responsible for coordinating the development and maintenance of information risk management policies, procedures and standards for the Council. The Council's SIRO is the Strategic Director of Resources.

The SIRO is responsible for the ongoing development and day-to-day management of the Council's Risk Management Programme for information privacy and security. The SIRO shall provide periodic reports and briefings to the Audit and Accounts Committee on information risk management developments

Information Asset Owners (IAO) are individuals involved in running the relevant service area with responsibility for understanding and addressing risks to the information assets they are responsible for. In the event of uncertainty, clarification and guidance should be sought from the Information Governance Manager. IAOs shall ensure that an information risk assessment is carried out on all information assets where they have been assigned 'ownership', following guidance from the SIRO / Information Governance Manager on assessment method, format, content and frequency. An account of residual risks should be included in the Risk Register of the relevant Departmental Business Plan).

The SIRO and Information Governance Manager will work closely with HR and the Communications team to ensure that appropriate actions are taken to provide staff with adequate training and education in order that they can fulfil their requirements to implement, maintain and develop effective information management controls.

Information Asset Administrators (IAA) are operations staff with the day to day responsibility for managing risks to their information assets.

Members and employees should question procedures, protocols and events that they consider could cause damage, harm or distress, result in a compliance breach or bring the Council's name into disrepute. By reporting incidents it allows the Council to highlight any areas of vulnerability, identifying where greater awareness is needed, or where procedures / protocols require reviewing.

Compliance and monitoring of the Information Risk Policy

The Head of Governance & Assurance is responsible for monitoring compliance with this policy.

If employees knowingly do not comply with Council policies, procedures or guidelines, the Council may take appropriate action under the Disciplinary and Dismissals Procedure.

Information

Further information and the most up to date policies and procedures on information management, risk management, information security and information governance can be found on iDerby/Governance/Information Governance.

Evaluation and review

This Policy will be reviewed by December 2016.

Help messages

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

Appendix 1

L1 **Information Governance Framework**

L2 **Information Governance Management**

L3 IG Strategy document
Information Governance Board TOR
Information Asset Register
Serious incident Reporting Policy
Information Risk 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
Mobile computing
Code of Connect compliance documentation
User access management policies

L2 **Action Plan**