



Derby City Council

Appendix 3

# Information Management Strategy

V1.0

## Information Governance Framework IGF/IGML3

Document owner	Richard Boneham, Head of Governance & Assurance on behalf of Strategic Director of Resources
Document author	Nick O'Reilly/Alison Moss
Document manager	Alison Moss, Information Governance Manager
Approved by and when	
Date of document	March 2013
Version	V1.0
Document classification	Public
Document distribution	Internal
Document retention period	Until date of next review
Location	TBA
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.**

<b>Date Issued</b>	<b>Version</b>	<b>Status</b>	<b>Reason for change</b>
March 2013	0.1	Draft	New strategy document
April 2013	0.2	Draft	Amendments and updates to first draft
April 2013	0.3	Draft	Incorporation of comments and updates from NOR
June 2013	1.0	Issued	Sign off 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

**CONTENTS**

1. Key Principles..... 4  
2. Corporate Approach ..... 5

DRAFT

## 1. Key Principles

- 1) Derby City Council will only collect, process and store information we need to fulfil our obligations and duties.
- 2) Derby City Council will comply with relevant legislation in respect of how we manage information and we will comply with the relevant codes of compliance and guidance issued by relevant authorities including the Information Commissioner's Office.

<http://www.legislation.gov.uk/>

<http://ico.org.uk/>

- 3) Derby City Council recognises that we hold a duty of trust to the citizens and businesses that we hold information about and undertake to protect the confidentiality, integrity and availability of this information.
- 4) Derby City Council will allow both individuals and businesses to access records we hold about them to check for accuracy, correct any errors and to keep information up to date except where such information is restricted in accordance with legislation or codes of compliance. Where licences permit this and where we can verify the identity of the individual through on line security measures we may provide access electronically from the Internet.
- 5) If a subject access request is made to access information either held in paper format or electronically by Derby City Council, we will only disclose information to the data subject or to a person authorised by the data subject to act on their behalf. The council will verify the identity of the person making the request and may charge the prescribed fee before disclosure is made.
- 6) Derby City Council may share data with other organisations where it is necessary to do so to fulfil our obligations or there is a legal requirement to do so. Where relevant Derby City Council will comply with published guidance and codes of practice on information sharing. Where information is regularly shared with external organisations an Information Sharing Agreement will be in place that will document the legal basis for the sharing.
- 7) Derby City Council will publish data via our website or by other means where we have an obligation to do so – including the [European Union Directive 2007/EC](#) known as [INSPIRE](#) and government requirements for transparency and open data including information covered by the [Freedom of Information Act 2000](#) and the [Environmental Information Regulations 2004](#). Data published in this way will be corporate information, including information such as performance measures, service targets, expenditure, census data or data shown in a spatial context. It will be anonymous or aggregated to protect personal information except in circumstances where legislation allows us to do so or tells us we must – for example senior management salary information, public registers and planning applications. Information published by us may be covered by copyright or licence restrictions and we may offer reuse on a

licenced basis.

- 8) Derby City Council has adopted record retention, archiving and deletion policies in accordance with relevant guidelines and will review information periodically to make sure it is not kept for longer than is necessary.
- 9) Derby City Council will adopt protective marking to relevant information in accordance with the UK government's regulations and framework covering protective marking.
- 10) Derby City Council will apply nationally agreed standards to the format and structure of information both to foster efficient management of information and to avoid minimising the risk of inaccurate or inconsistent data being used.
- 11) Derby City Council will publish Privacy Notices at the point of collection of personal information and make them readily available. Privacy Notices will say why we are collecting information and who we will share it with and may give the option for citizens to opt out of data sharing unless to do so would be a breach of our obligations. We will only process information in line with the Privacy Notice or seek consent if a further sharing requirement is identified and to do so without consent would be a breach of Principle One and Principle Two of the [Data Protection Act 1998](#).
- 12) Derby City Council will only combine personal information held for specific purposes with consent from data subjects or where there is a legal or statutory requirement to do so or where an exemption allows this to happen in law. Whenever the Council intends to combine different sets of personal information Privacy Notices will be published that will state the purpose for any combination and if applicable will provide an opt-out at that time – unless to do so would prejudice the crime prevention exemption of S29 (1) and/or (2) of the Data Protection Act 1998.
- 13) Derby City Council provides advice, guidance and training to all staff involved with managing information before they are allowed to work with personal information. This varies depending on the nature of the information each employee will have access to in the course of their duties. Breach of Information Management and/or Information Security policies and procedures may be subject to disciplinary action under the Council's code of conduct.

## **2. Corporate Approach**

- 1) The Council will adopt a corporate approach to Information Management to help make sure of both effective use and to minimise the amount of duplication and potential inconsistency.
- 2) As part of this corporate approach the Council will develop and maintain a corporate Information Asset Register which will record the different information we hold, the sources of the information and any internal or external information work-flows. This will include links to the currency of the information and any

regular requirements to check, update, archive or delete the information.

- 3) Derby City Council has identified Information Asset Owners in all Departments who will be primarily responsible for the production of the Information Asset Register and the application of policies and procedures that govern the management of information they are responsible for.
- 4) Derby City Council has adopted a corporate Information Governance Framework, that this Strategy falls within to manage information security, confidentiality, integrity and availability.
- 5) The council has appointed a number of senior managers to be responsible for Information Management:
  - a. A Senior Information Risk Owner (a member of the Chief Officer Group)
  - b. Caldicott Guardians for both Adult and Children's services
  - c. A Director of Information Systems to make sure we are compliant with relevant technical security
  - d. An Information Governance Manager responsible for managing and monitoring policies and procedures within the information governance framework
  - e. Information Asset Owners in each department responsible for specific information records (data-sets)
- 6) The Council is adopting a Master Data Management strategy which will be used to move towards a single view of our customers and in doing so means we will be applying common and consistent use of validated address records. This will include facilities to map data from different systems to identify where we hold multiple and potentially inconsistent or out of date information and to correct it. The sole purpose of data mapping will be to improve the accuracy and consistency of information the Council holds and is responsible for. As part of the strategy the Council intends to move towards...
  - a) a single consistent address to avoid inefficiency and inconsistency of data and to support single notification of change of address.
  - b) a single customer reference which can be used together with different customer references needed for different purposes (NHS Number, Patient number, Council tax Reference). Where we adopt a single customer reference knowledge of this reference will not allow access to sensitive and confidential data without separate authentication.
- 7) The Council may from time to time undertake other data mapping exercises, where it is lawful to do so and where there is a benefit to the Council and the data subjects in fulfilling our obligations. Where data mapping is to take place a statement of purpose will be agreed and published documenting what data is being mapped, for what purpose and what safeguards will be applied.
- 8) When data mapping exercises take place no employee or agent of the Council will be given access to information that is personal or sensitive from a data set

they would not normally access. Social care and health records that the Council hold may be mapped to check identity but any specific information on health, finances or care provision will remain restricted to employees who have a genuine need to access this information.

- 9) The Council will use a number of corporate information systems as a basis for Master Data Management. These will include:
- a. Revenues and Benefits as a key source of person and household data about adults
  - b. Social Care databases as a source of person data on both adults and children
  - c. Schools databases as a source of person data about children
  - d. Land and Property Gazetteer as the prime source of address data for properties within the City boundary
  - e. Customer Relationship Management as a tool to record and maintain a unique customer reference which can be shared with other systems
  - f. Electronic Document and Records Management as a tool to store protectively marked documentation in a secure and controlled environment
  - g. Geographical Information System as a source of spatial data and a tool to link relevant information in a spatial context.
  - h. Service specific databases such as planning, library management, leisure bookings which support customer transactions.

Where these information systems are used to collate Master Data Management each system and each Information Asset Owner will maintain its own controls on what information is extracted.. These will include

- frequency of extraction, and
  - what rules will be applied to updating originating system with corrected information.
- 10) The Council will not duplicate or copy specific information (such as health records) between systems unless there is a clear legal requirement to do so. We will not include any information in the Master Data Management system which it is prohibited from being used in this way.
- 11) The Master Data Management solution will be used as a tool to improve and maintain data accuracy and quality and to avoid the need for multiple notifications of core information such as name or address change, or notification of a death. It will not be used to manage or deny access to Council services where a citizen or business has a legal right of access.
- 12) Only anonymised or pseudoanonymised information will be used when the Council analyses information on the pattern or use of different Council services by different customer groups. Analysing data in this way can be an important tool in reviewing and planning service delivery but we will always make sure that the prime duty of confidence and trust is an over-riding priority.