DATA MATCHING POLICY & STRATEGY
Version 1.0

Document Owner	Richard Boneham, Head of Audit & Risk Management
Document author and enquiry point	Paul Needham, IT Auditor
Review date of document	2009
Version	v1.0
Document classification	Internal
Document distribution	Internal
Document retention period	Until date of next review
Next document review date	2009

Document Review: TBC

Section	Title	Addition or change	Reason

Contents:

<u>Data Matching Policy</u>

1. Introduction & Scope

1.1. Derby City Council is committed to the prevention, detection and investigation of all forms of fraud and corruption. Continuous Auditing will act as a pro-active approach to identifying and where possible preventing fraud and corruption.

1.2. The benefits of data matching can be seen through initiatives such as "The National Fraud Initiative", which is the Audit Commission's Data Matching exercise that is setup to tackle numerous fraud activities within the public sector. Data Matching under the National Fraud Initiative is a legal requirement.

1.3. Targeted internal data matching, analysis and exception testing may identify more areas for further investigation, or "hits", than the NFI exercise. This may lead to both investigation work through identifying potential fraud, as well as giving us the chance to develop Systems Assurance work.

1.4. Performing a Data Matching and Data Analysis process internally, and informing people that we are performing this process internally, may act as a successful deterrent by creating an anti-fraud and corruption culture within Derby City Council.

2. Definitions

2.1 Data Matching – The computerised comparison of two or more data sets which relate to the same individual or element

2.2 Data Analysis – The process of transforming data in the aim to extract some useful information and conclusions

2.3 Continuous Auditing – The method that is used to perform control and risk assessments in an automated manner on a more frequent schedule

3. Purpose of Policy

3.1 Derby City Council will adhere to only match and analyze data within the appropriate legislative framework.
3.2 To ensure that a consistent approach to data matching is adopted throughout Internal Audit by adhering to clearly defined data matching strategy.
3.3 To establish procedures that ensure data matching is conducted in a controlled, robust and approved manner.

4. General Principles

4.1   The data we extract will only be obtained in accordance with the provisions of the Data Protection Act (1998).

4.2   Data subjects will be notified where required, that their data may be used in our exercises, for the purpose of fraud detection and prevention.

4.3   To ensure that data is processed fairly, our data matching technical approach will be such that it is indicative of fraud, and may be refined after experience.

4.4   The matching exercise results do not automatically imply that fraudulent activity is taking place; they simply indicate that there may be a need for an investigation. We will ensure that our investigation team undertake thorough reviews of all results. This will serve the dual purpose of establishing innocent findings and will also allow us to refine the data matching process for future use.

4.5   The data we will extract will be relevant and the minimum required for undertaking our exercise and reporting on the results.

4.6   At the end of any periodic exercise, i.e. monthly exercise, the output data will not be held for any longer than is required for the purpose of the exercise.

4.7   Data will be securely stored throughout the exercise.

5. Training

5.1   All relevant staff receives appropriate training to provide assurance that the policy is understood and adhered to.

6. Approval

6.1   This policy has been created in consultation with the Corporate Director for Resources, the IT Security/Data Protection Officer, the Audit and Accounts Committee and our legal representatives.

7. Implementation

7.1   The Head of Audit and Risk Management will be responsible for ensuring that this policy is implemented.

8. Data Retention & Disposal

8.1   Data retention/disposal standards will be established within Derby City Councils records management policy

8.2   Personal information will be safeguarded against accidental or malicious threats to confidentiality and integrity.

9. Other Relevant Policies

9.1   [Information Security Policy](#)

9.2   [Data Protection Policy](#)

Data Matching Strategy

1. Introduction

1.1   It is one of Internal Audits key objectives to achieve greater pro-active anti-fraud work. This requires us to make better use of information available to us to improve our service delivery. External key drivers for our Data Matching and Continuous Auditing work include the Audit Commissions KLOE (key lines of enquiry) for the Use of Resources, our new external auditors are keen on pro-active fraud work, and the Government is keen on Local Government to use information and intelligence more effectively to help eliminate fraudulent activity.

1.2   We see the potential to expand the Data Matching exercise to any system within our authority, and also to enhance to exercise by using data from other local authorities. To support this work we have dedicated resources within the department to develop a data matching and continuous auditing program.

2. Goals & Objectives

2.1   Derby City Council is committed to the prevention, detection and investigation of all forms of fraud and corruption. Continuous Auditing would act as a pro-active approach to identifying and where possible preventing fraud and corruption.

2.2   The key goals and objectives of the strategy are:

- Provide an effective internal control and a means of helping to prevent or identify fraudulent or corrupt activities.

- Develop an internal tool to help identify errors, inconsistencies, irregularities and risk to financial resources within Derby City Council.

- Ensure that we are fully utilising the data held within Derby City Council's financial systems to best possible effect.

- Aid the audit planning process and other audit projects.

- Improve the control environment within Derby City Council.

- Identify potential weaknesses in design and operation of internal controls that may inadvertently be creating the risk of fraud or irregularities occurring.

- Identify potential weaknesses in the design of Information Systems that currently may not provide adequate assurances that they will prevent error or fraud.

- The key lines of enquiry for use of resources 2008 assessments from the Audit Commission state "The council undertakes proactive counter

fraud and corruption work which is determined by a formal risk assessment."

3. Scope of Data Matching

3.1.   Data analysis and matching may be performed on any system within Derby City Council.

3.2.   Looking forward, we may develop this strategy to incorporate matching and analysis of data between authorities and other organisations.

3.3   Data matching will be performed routinely as part of our data matching plan, and also on an ad-hoc basis:

Routine – matches may take place on a daily, weekly, monthly or quarterly basis in line with our data matching plan.

Ad-hoc – one off data matches may be required for scenarios when the routine data matching plan would not be appropriate. This could also include extractions to aid the audit of large information systems.

4. Legal Basis for Data Matching

4.1.   In order for Derby City Council to pursue our proposed Data Matching / Continuous Auditing process it is essential that we work within the relevant legislative framework. We will actively work with the Data Protection Manager and Legal Department to ensure we set up the correct legal procedures to drive improvement within Derby City Council.

4.2   For all new legislation or amendments to existing legislation, we will seek the relevant legal advice and advice of the Data Protection Manager to ensure we are working with the correct legislative framework.

4.3   We will adhere to the Data Protection Act by ensuring there are the relevant fair processing notices in place to inform the data subjects that this exercise is necessary to help detect and identify fraud.

5. Approach to Data Matching

5.1   A risk assessment process will be performed to formulate a risk determination to help us target areas with a high risk profile. This process will allow us to formulate an annual data matching plan. Our plan will cover both routine data matches, whilst leaving the plan flexible enough to include ad-hoc data matches where necessary.

5.2   For all our proposed data matches and exception tests a justification process will be conducted with the relevant Departmental Data Protection Liaison Officers and System Owners. This involves specifying our data requirements and field definitions, and creating a justified key objective that details what the test may identify.

5.3   All future proposals of Data Matches and Exception Testing will follow the same justification process.

5.4   The overall approach to Data Matching involves an extraction of data from any system or data warehouse within our authority, and then subsequently cross matching or exception testing this data to another data set to help identify potential errors, irregularities or suspect matches. Section 10 of this strategy details our proposed set of tests and matches.

6. Retention of Data

6.1   We will ensure that data is not kept for longer than necessary in order to perform our specified analysis. Retention and archiving periods will be considered in line with on going Document Retention Schedules.

6.2   Data matches, analysis and testing that indicate potential fraud or areas for further investigation will be retained in line with investigation procedures.

6.3   We will retain only two generations of each data extraction, to prevent duplication of work investigating a discrepancy which was reported in the last cycle of extractions and which was resolved in the past.

6.4   Our planned data extraction frequency means that existing data extractions will replace previous extractions. Where a new extraction has been conducted to replace existing data extractions, the previous data will be securely deleted and replaced by the new extraction.

7. Storage of Data

7.1   Data that is created from extractions, analysis, testing and cross matching is held in secure files with restricted access.

7.2   Data that does not indicate a match or does not need to be retained for further investigation will be securely removed.

7.3   We have no existing plans to match paper based records. In exceptional circumstances where this in necessary, we will ensure manual records are stored in securely in locked cabinets.

8. Links to Audit Controls and Risk Registers

8.1.   Where significant fraudulent activities have occurred through poor system controls, the details will be:

        a)   entered into the relevant risk register, and
        b)   included in a follow-up framework

        This will allow the measures taken in response to be assessed as to their effectiveness. The follow-up may be carried out as part of the next

timetabled audit or may be given greater urgency, depending on the nature of the activities. In either case, the follow-up would take place as a separate exercise to the data-matching process.

8.2.   Details will be recorded on our Internal Audit Management systems to help assess the implications on the annual assurance statement and for future trend analysis.

9. Management Action

9.1   The Audit Manager will make arrangements for follow-up of all positive data matches where a fraud has occurred but no action has been taken against the perpetrator(s) of the fraud.

9.2.   If no action is taken by a line manager when a fraud or irregularity is proven, the Head of Audit and Risk Management reserves the right to review the fraud circumstances and refer the matter to the Audit & Accounts committee.

Appendix 1

We recognise the importance of ensuring that data extracted through this process is stored securely. Arrangements are being put in place with the Head of Strategic Infrastructure to ascertain the security status of an existing SharePoint server outside the control of the Council's ICT contractor
This server is currently being used as a project office for documentation and collaborative working on the current review of the ITSP contract. This will therefore not involve the Council in any additional expenditure.

Appendix 2

Sample of Matches and Tests to be carried out

The following are examples of the type of matches to be carried out.

System	Name	Objective
Creditors	Duplicate VAT Registration Number	To extract all creditors that have the same VAT number as all VAT numbers are unique
Council Tax	Accounts for each council tax banding	Ensure that the correct debit has been raised for the properties in each band
Housing Benefits	Sample with an overpayment indicator	Ensure the claimants have either a sundry debtor account or that it is being recovered through benefit
Payroll	Employees with no tax code	To identify any records with no tax code
Payroll	Pension scheme	To extract records where employees over 65 or under 16 are contributing to the pension scheme
Housing Rents	Right to Buy	To confirm that people on the right to buy list are sitting tenants