

Local Government Improvement & Development  
Managing Local Performance

**A tool kit for**  
**Data Quality**

December 2010

# A Data Quality Toolkit

## CONTENTS

Introduction .....	2
The risks of failure due to poor quality data .....	2
<i>Who depends on reliable data?</i> .....	2
<i>The risks of ignoring data quality - why should we treat data quality seriously?</i> .....	3
<i>Factors which contribute to poor quality data and information</i> .....	3
1. Culture .....	3
2. People .....	4
3. Processes .....	4
What do we mean by data quality?.....	5
<i>Data, information, knowledge – what is the difference?</i> .....	5
<i>Key characteristics of good quality data</i> .....	5
1. Accuracy.....	5
2. Validity .....	5
3. Reliability .....	5
4. Timeliness .....	5
5. Relevance.....	6
6. Completeness .....	6
Essential elements for producing good quality data.....	6
<i>Commitment from the top – the importance of leadership</i> .....	6
<i>Who is responsible for data quality?</i> .....	7
<i>Data quality policies &amp; procedures</i> .....	8
<i>Learning from others – the value of networking and collaboration</i> .....	9
<i>Skills, training and updating</i> .....	9
<i>Role of IT in enhancing data quality</i> .....	10
<i>Assurance and validation mechanisms</i> .....	11
Accessing data - record naming conventions .....	12
Data sharing.....	13
<i>Data sharing and geographical information systems</i> .....	15
<i>Data sharing for benchmarking</i> .....	16
<i>Data sharing protocols</i> .....	16
Data protection – myths and realities .....	17
Data handling – the risk of misplaced or lost records .....	18
Data security – the risk of unlawful or malicious attack .....	19
The future? .....	19
Further Information.....	20
Acknowledgements .....	20

### Document history:

Version 1	25/11/10	First draft
Version 2	30/11/10	Additions & revisions - sent to AB, LGID
Version 3	06/12/10	Consultation draft produced
Version 4	09/12/10	Further additions following consultation on case studies

## Introduction

The idea for this toolkit emerged from discussions following the publication of the Audit Commission report, “*Nothing but the truth?*” in November 2009. The essential idea is to provide assistance to those wishing to improve data quality through practical tips and examples of good practice in councils as well as providing a digest of the findings of a series of reports published by the Audit Commission and other bodies (see “[Further Information](#)” section at the end of the Toolkit).

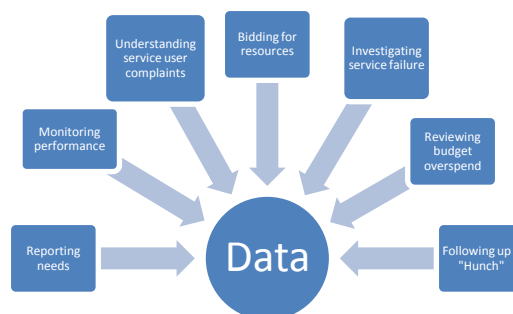
The risks that we face if we do not have accurate, timely and understandable data are considerable. Virtually every high profile failure in local government can be traced, in varying degrees, to this very factor. With this in mind, we have produced this simple toolkit to assist those wishing to ensure that they can have confidence in the data that they need for their duties. For some, data quality relates to the data underpinning those performance indicators required by central government and auditors. This toolkit takes a much wider view of the term – as data is an essential ingredient to the delivery of good service to local citizens who pay for, and use, those services.

The literature on the key components of data quality – and indeed of data protection, security and sharing – all point to the same important features of good management practice. This toolkit aims to set out, in a concise way, those features and suggest methods for achieving them.

Before exploring these, however, we need to be clear on what we mean by the various terms we all use so regularly but so often in very different ways from each other. We also need to consider the risks of not treating data quality seriously

## The risks of failure due to poor quality data

We need to consider just how vital to the delivery of public services is accurate and timely data and its analysis. This diagram identifies a range of situations where people require robust quality data to make decisions or to pursue a course of action. Data on performance goes beyond the responsibility of the specialist officer charged with submitting returns to a government department. Data is vital to allow the organisation to focus on what needs to be done, to provide evidence to support decisions and to evaluate the effectiveness of all aspects of a council’s operation.



## Who depends on reliable data?

We also need to consider the wide range of “customers” for the data that our organisations generate:

- Government – to provide the evidence base for legislation, policy development and budget planning
- Local government – to provide an overview of community needs, service user experience, service performance and ensure the efforts of different services and professions are joined up.
- Partners - to provide the evidence base for shared strategies (e.g. Sustainable Communities Strategies) and joint planning (e.g. in health or community safety)
- Service Managers – to account for the performance of their section and to drive improvement
- Frontline staff - to perform duties, to serve the public and to detect errors or failures in order to improve the service they offer
- Public - as service users (so that they can understand what service they should expect) and as service funders (so that they can understand how their taxes and charges are being spent)

The requirements of submitting data to external bodies (Government, auditors, inspectors) seems, in recent times, to have eclipsed the needs of the local authority and its own requirements.

*“Data generation should be a by-product of normal business, not an end in itself. The starting point should be ‘what data does the frontline need to deliver its business well, and for us to know that is happening?’”*

*(Nothing but the truth? Audit Commission)*

We need to consider what quality data need to be, so that data is sufficient for the purpose for which it is collected. Decisions that affect the cost, quality and effectiveness of public services must be underpinned by robust information. Councillors and senior management teams complain of lengthy reports yet do not have the relevant information they need. This can be overcome without spending more by deploying existing resources more wisely. According to the Audit Commission (*Is there something I should know?*), 36% of analysts' time is spent on routine performance reporting, while only 15% is spent on value added analysis. Decision makers need to become more demanding, and analysts more valued.

### ***The risks of ignoring data quality - why should we treat data quality seriously?***

The high-profile failure of public authorities to safeguard Baby Peter in Haringey, Fiona Pilkington in Leicestershire (see section on “Data Sharing”) and to prevent the high number of deaths in Mid- Staffordshire NHS Foundation Trust, has directed attention to the accuracy and reliability of the data underpinning local service delivery. It is not a matter of quantity; there is more data about services than authorities can realistically use..

*“A 2005 Cabinet Office report, quoted by Sir David Varney, charts the 44 contacts over 180 days a bereaved family had with public bodies to update their records. Even after the 180 days, many issues had still not been resolved. As part of its assessment of how well the bodies it audits use their resources, the Audit Commission looks at whether they have arrangements in place to ensure good data. In the most recent assessment, fewer than 5 per cent of local authorities had excellent arrangements, while 12 per cent of performance indicators that we tested were of such poor quality as to be inadmissible.”*

*(Nothing but the Truth, Audit Commission)*

Responsibility for the quality of data unambiguously rests with the organisation producing it.

### ***Factors which contribute to poor quality data and information***

Over a considerable period, the Audit Commission, after looking at the quality of data in local councils, health trusts and fire and police authorities, identified a number of reasons for poor data quality which were common across different sectors:

#### **1. Culture**

##### ***Complacency and lack of leadership***

Senior managers, non-executive directors and elected members often take for granted the quality of the data their organisation produces, and fail to scrutinise it.

##### ***Lack of accountability and engagement of staff***

Data quality is often not at the heart of day-to-day operations, and a common obstacle to achieving consistently high-quality data is the perception that this is not an important part of a person's job. Responsibility is commonly delegated to a specialist, rather than across agents in the data chain. The Audit Commission (in *“Is There Something I Should Know?”*) reported that those at the aggregating or reporting stage sometimes spend 80 per cent of their time on data quality problems that should, and could, have been rectified earlier. Data quality improved when front line staff and supervisors were involved in designing systems and processes, and understood that important outputs of a service (e.g. payments to suppliers) could be seriously affected if data was poor.

### *Insufficient incentives to improve data quality*

However, those gathering data are typically not the users of it. Incentives therefore need to be built in for both individuals and departments to improve data quality. Members of staff across the data chain should have data quality incorporated into their personal performance objectives. In addition, local public bodies should take time to think how they could more fully exploit the data that they have.

## **2. People**

### *Insufficient training and development for staff and board members*

The Audit Commission's "*Figures You Can Trust*" report highlighted that board members may not have the knowledge and expertise to ask the right questions and to challenge on data quality. Their assessment of NHS waiting lists concluded that inadequate training for staff contributed to poor data quality, a finding echoed in reviews of information management and governance in NHS trusts.

### *Poor quality source documentation*

Following the Baby Peter case, the special Joint Area Review of the London Borough of Haringey in November 2008 found that *'the standard of record keeping on case files across all agencies is inconsistent and often poor... Police and health service files are often poorly organised and individual cases are difficult to follow. Health services files include hand-written notes which are sometimes illegible and do not identify the author. The standard of record-keeping in the health records of looked-after children and young people is poor and some entries are inaccurate'*.

The Commission for Social Care Inspection found something similar whilst investigating the quality of care practice with people experiencing abuse. "*Case recording was criticised in over half of inspections. When a number of staff or agencies are involved in supporting someone who has experienced abuse, good recording is necessary for continuity of support.*"

### *Inconsistent recording and inputting*

Even when the right policies and procedures are in place, people still have to follow them. For example, to produce reliable and comparable data on racial incidents and anti-social behaviour, police need to record the status of a caller as a victim, witness or third party. Yet in Audit Commission reviews of police authorities it was found that staff within the same force recorded events differently – as did different forces.

## **3. Processes**

### *Inadequate policies and procedures*

A common finding in Audit Commission reviews of data quality in local government has been the lack of robust policies and procedures both corporately and, more commonly, at service level, to ensure good quality data. This can lead to different assumptions being made by different people producing figures at the same level in the data chain.

### *Ineffective ICT*

In over half of the health trust sites that the Audit Commission checked for waiting list accuracy, ineffective or poorly configured and integrated ICT systems contributed to mistakes. Often the wrong date would be entered as the ICT system had been programmed to default to the date the entry was made.

### *Lack of integration into risk, performance and financial frameworks*

Police authorities improved their data quality when it became a mainstay of financial, performance and risk management. Research on data quality in the NHS confirms that *'where trusts had identified the quality of data as a risk, its prominence at board level and subsequent discussions increased'*.

## What do we mean by data quality?

### *Data, information, knowledge – what is the difference?*

The Audit Commission suggested the following definitions:

Data	Data are numbers, words or images that have yet to be organised or analysed to answer a specific question.
Information	Produced through processing, manipulating and organising data to answer questions, adding to the knowledge of the receiver.
Knowledge	What is known by a person or persons. Involves interpreting information received, adding relevance and context to clarify the insights the information contains.

(*Improving information to support decision making: standards for better quality data* Audit Commission)

It is often said that organisations are “data rich but information poor”. In truth, there is a close relationship between data, information, knowledge and wisdom. This is the key to understanding both the need for data and the importance of quality of data.

### *Key characteristics of good quality data*

This section will explore what we mean by **quality** as it applies to data. Quality in the delivery of services is usually expressed as “value to the user” or as “fitness for purpose”. In other words, we can only really describe data as possessing quality if the users of that data consistently find that it serves their needs.

The Audit Commission (in *Improving Information to Support Decision Making: Standards for Better Quality Data*) identified six key characteristics of good quality data:

#### **1. Accuracy**

Data should be sufficiently accurate for their intended purposes, representing clearly and in enough detail the interaction provided at the point of activity. Data should be captured once only, although they may have multiple uses. Accuracy is most likely to be secured if data are captured as close to the point of activity as possible. Reported information that is based on accurate data provides a fair picture of performance and should enable informed decision making.

The need for accuracy must be balanced with the importance of the uses for the data, and the costs and effort of collection. For example, it may be appropriate to accept some degree of inaccuracy where timeliness is important. Where compromises are made on accuracy, the resulting limitations of the data should be clear to their users. This must be a judgement determined by local circumstances, and is unlikely to be appropriate in the case of the data supporting published performance indicators.

#### **2. Validity**

Data should be recorded and used in compliance with relevant requirements, including the correct application of any rules or definitions. This will ensure consistency between periods and with similar organisations, measuring what is intended to be measured. Where proxy data are used to compensate for an absence of actual data, bodies must consider how well these data are able to satisfy the intended purpose.

#### **3. Reliability**

Data should reflect stable and consistent data collection processes across collection points and over time, whether using manual or computer based systems, or a combination. Managers and stakeholders should be confident that progress toward performance targets reflects real changes rather than variations in data collection approaches or methods.

#### **4. Timeliness**

Data should be captured as quickly as possible after the event or activity and must be available for the intended use within a reasonable time period. Data must be available

quickly and frequently enough to support information needs and to influence service or management decisions.

## 5. Relevance

Data captured should be relevant to the purposes for which they are used. This entails periodic review of requirements to reflect changing needs. It may be necessary to capture data at the point of activity which is relevant only for other purposes, rather than for the current intervention. Quality assurance and feedback processes are needed to ensure the quality of such data.

## 6. Completeness

Data requirements should be clearly specified based on the information needs of the body and data collection processes matched to these requirements. Monitoring missing, incomplete, or invalid records can provide an indication of data quality and can also point to problems in the recording of certain data items.

Return to [Table of Contents](#)

## Essential elements for producing good quality data

This section puts forward management arrangements that authorities can put in place to secure the quality of the data they use to manage and report on their activities. These are derived from a number of sources, including the Audit Commission's standards set out in *Improving Information to Support Decision Making: Standards for Better Quality Data*. This section explores the following themes:

- Commitment from the top – the importance of leadership
- Who is responsible for data quality?
- Data quality policies & procedures
- Skills, training and updating What about staff who are too busy or unwilling to change?
- Learning from others – the value of networking and collaboration
- Role of IT in enhancing data quality
- Assurance mechanisms
- Data use and reporting - the arrangements and controls in place for the use of data

### *Commitment from the top – the importance of leadership*

The most important component for ensuring quality of data is that there is commitment from the top management team of the organisation. Without this, all the other components are very unlikely to be effective. A council needs to put in place a corporate framework for management and accountability of data quality, with a commitment to secure a culture of data quality throughout the organisation.

The ways this can be demonstrated include:

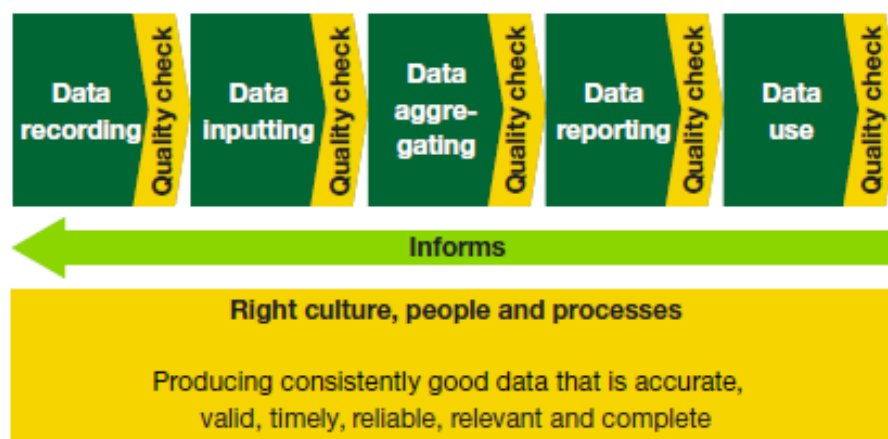
- A senior individual at top management level (for example a member of the senior management team) has overall strategic responsibility for data quality, and this responsibility is not delegated.
- The corporate objectives for data quality are clearly defined and agreed at top management level, published and circulated throughout the organisation.
- The data quality objectives are linked to business objectives, cover all the body's activities, and have an associated delivery plan.
- The commitment to data quality is communicated clearly, reinforcing the message that all staff have a responsibility for data quality.
- Data quality is embedded in risk management arrangements, with regular assessment of the risks associated with unreliable or inaccurate data.
- Where applicable, the authority has taken action to address the results of previous internal and external reviews of data quality.
- Where there is joint working, there is an agreement covering data quality with partners (for example, in the form of a data sharing protocol, statement, or service level agreement).



## Who is responsible for data quality?

There needs to be a clear allocation of responsibilities and the temptation to view data quality and information management as information technology (IT) issues must be avoided.

Producing and using good quality data entails having the right culture, people and processes to support it. At each stage in the data chain, from initial recording to its ultimate use, local public bodies should have a means of systematically assuring the quality of their data. This could take the form of internal audits, peer scrutiny, automated checking for unexpected inconsistencies and variances, carefully set-up systems (such as self-righting systems) or senior management sign-off.



*“The quality of data should be assured as close to the point of origin as possible. Errors get more difficult to detect and rectify as data moves along the chain and out to other organisations, whether reported from a council or health trust to a local strategic partnership or a government department. Mistakes can become compounded and data may well have already been used to make key decisions by the time the errors are noticed.”*

*(Nothing but the truth? Audit Commission)*

A common obstacle is the perception that this is not an important part of a person’s job. Staff who record data need to see the benefits for their effort in securing the quality of that data. This can be achieved by, for example, ensuring these staff receive the relevant performance information in return and by regular sessions bringing together those using the data with those responsible for generating it.

The ways this can be demonstrated include:

- Accountability for data quality is clearly defined, documented and incorporated into job descriptions.
- Implementation is considered as part of the performance appraisal system.
- There is a framework in place to monitor and review data quality, with robust scrutiny by those charged with governance.



### Case study

Bolsover District Council's Data Quality Management Statement (2007) sets out the roles and responsibilities for all sections of the Council thus:

#### Roles and Responsibilities

All departments within Bolsover Council have the responsibility to deliver the objectives within this statement, however specific responsibilities are as follows:

- The **Head of Customer Service and Performance** has Senior Officer responsibility for Corporate Data Quality and is Officer Data Quality Champion.
- The **Portfolio Holder for People and Performance** is the Elected Member Data Quality Champion.
- **Senior Management Team** has the overall responsibility to oversee and monitor the collection of financial, performance and other data.
- **Senior managers and officers** will have an active role in collecting and organising the information. They will ensure that designated officers calculate and input data from source information systems into PERFORM (computerised performance management system). Managers will also communicate the 'collective responsibility' for data quality. Heads of Service will ensure that there is at least one other officer capable of calculating and inputting data from source

### Data quality policies & procedures

Authorities should put in place appropriate policies and procedures to secure the quality of the data it records and uses for reporting.

These policies and procedures should

- provide guidance for staff on data quality, in the form of operational procedures, covering data collection, recording, analysis and reporting for all business areas.
- include relevant national regulation and guidance, (e.g. on the Data Protection Act and the Freedom of Information Act) as well as the organisation's own arrangements
- be applied consistently and monitored regularly. Mechanisms should be put in place to check compliance with corrective action taken where necessary. Regular reports on this should be reported to top management.
- be reviewed periodically and updated when needed.
- Incorporate arrangements to inform staff promptly of any policy or procedure updates

All relevant staff should have ready access to these policies and procedures.

### Case study

Suffolk County Council 's approach states that data quality is everyone's responsibility; effective implementation of its policy will impact positively on all staff and raise the quality of data available for business decision-making. "The benefits of improving the quality of the data will ensure that:

- we hold robust and reliable data for strategic decision-making;
- we have the most reliable client or service data on which to base operational decisions;
- we retain accurate HR and financial records;

#### Suffolk County Council Data Quality Policy

##### CONTENTS

Outline – 'our commitment'	3
Defining quality	4
Scope	4
Effective governance & leadership: roles & responsibilities	4
Staff training, awareness and appraisal	5
Reviewing data quality	6
Documentation and sharing best practice	6
Third party data	6

- we have a comprehensive picture of the state and accuracy of all our data to facilitate sharing with partners.”

It reviewed and revised its Data Quality policy in March 2010. This comprehensive document covered all the key aspects of assuring data quality (see inset illustration) set out in this tool-kit:

### *Learning from others – the value of networking and collaboration*

All authorities are faced with the challenge of ensuring the quality of data. To avoid the danger of “re-inventing the wheel”, authorities could usefully find out what other organisations are doing in this field. There is a specialist web-based Community of Practice dedicated to Data Quality (<http://www.communities.idea.gov.uk/c/79131/home.do>) which is open to anyone in the sector.

There are also other, more local networks which aim to bring together all interested in the subject – and not just data or information specialists, such as London Data Connects.

#### **London Data Connects**

London’s Improvement and Efficiency Partnership, Capital Ambition, hosts a London-wide forum “**London Connects**” aimed at public sector staff actively involved in data management and sharing good practice and experience on:-

- Datasets used
- Accuracy of systems
- Accuracy of fields within systems
- Rules for matching
- Process for handling matched data
- Process for handling mis-matched data
- Data matching tools, middleware, partners used
- Corporate IT architecture
- Building up a picture of “trusted” data sources
- Links to National projects e.g. Tell Us Once, ContactPoint etc.

London Connects has commissioned a number of reports on behalf of the 33 London authorities including one on data quality (*Data quality management in local authorities, Tribal/London Connects June 2009*) which covers the issue of data quality for all types of information and provides local authorities with a framework on which they can develop their own data quality strategy.

### *Skills, training and updating*

Staff need to have the knowledge, competencies and capacity for their roles in relation to data quality. Training, coaching and supervision sessions should be based on the policies, procedures and standards outlined previously along with the clear signals about the importance of the subject from senior management.

The ways this can be demonstrated include:

- Data quality standards are set, and staff are assessed against these.
- The authority has put in place a programme of training for data quality, tailored to the needs of staff, to ensure they have the capacity and skills for the effective collection, recording, analysis and reporting of data. This includes regular updates for staff to ensure that changes in data quality procedures are disseminated and acted on.
- There are corporate arrangements in place to ensure that training provision is periodically evaluated and adapted to respond to changing needs.

## Case studies

Various authorities developed and shared their own in-house Data Quality workshops following discussion and collaboration on the **Data Quality Community of Practice** (<http://www.communities.idea.gov.uk/c/79131/home.do>).

Among these were Nexus (the Tyne & Wear Passenger Transport Authority), Pendle Borough Council and North Lincolnshire Council and Gravesham Borough Council.

Gravesham's workshop aims to be short (30 minutes or so) and covered:

- What is data?
- What is data quality and why is it so important?
- How is data used in this council?
- What does this all mean for me? (everyone has a role and a responsibility)
- Key documents
- Key contacts

### Aims of the session

- To clarify what we mean by 'data' and data quality
- To identify and give examples of the consequences of poor data quality
- To review what data quality means for Gravesham
- Key documents and contacts

Gravesham

What about staff who are too busy or unwilling to change? Authorities can be imaginative about ways to reach those unable or unwilling to attend training sessions.

#### Data Quality Tips of the day

**Awareness** – of the 'nuts and bolts' to collecting, recording and reporting good quality data.

**Collecting and recording data** – tips for improving data quality using IT.

Tonbridge & Malling Borough Council found, from a staff survey, that many felt that they lacked the skills, the IT resources and/or the time to keep good records or provide good quality data in relation to their day to day work. In response, over a period of six weeks, 30 tips were emailed to all staff at the rate of one tip per day. The tips were classified according to how they helped staff improve their knowledge and work and were kept short so staff could quickly discount those that don't apply to them or that they know about already.

## Role of IT in enhancing data quality

Information technology offers considerable scope for the consistent gathering, collation, sorting, checking and reporting of data and ensuring data quality.

### Case study

Brent Council invested in data cleansing software to assure the quality of data held in the council's central client Index, which matches data from the back-office systems that support the delivery of council services. Key datasets like postal and email addresses, phone numbers and gender are checked for consistency before the data is integrated into the Council's central hub. Major factors in the Council's decision to invest in this software were compliance with data protection requirements and also because good quality data enables better customer service provision. The software carries out the data cleansing processes and provides reporting metrics and dashboard features to demonstrate improvements in data quality to each council department.

Tony Ellis, Brent Council's Head of IT  
"We are able to use improvements in the quality of our data to deliver improvements directly in our levels of customer service, reduce our cost of contacting customers and reduce instances of fraud through consistency and greater transparency of our core systems data."

## Assurance and validation mechanisms

To provide themselves and the wider public with assurance that their data is reliable, councils need to put in place systems and processes which secure the quality of data as part of the normal business activity of the body. The Audit Commission report *Improving Information to Support Decision Making: Standards for Better Quality Data* includes the following key elements to demonstrate this:

- Systems and processes are in place for the collection, recording, analysis and reporting of data which are focused on securing data which are accurate, valid, reliable, timely, relevant and complete.
- Systems and processes working according to the principle of right first time, rather than employing extensive data correction, cleansing or manipulation processes to produce the information required.
- Arrangements for collecting, recording, compiling and reporting data which are integrated into the business planning and management processes of the body, supporting the day-to-day work of staff.
- Information systems with built-in controls to minimise the scope for human error or manipulation and prevent erroneous data entry, missing data, or unauthorised data changes. Such controls should be reviewed at least annually to ensure they are working effectively.
- Corporate security and recovery arrangements are in place. The body regularly tests its business critical systems to ensure that processes are secure, and results are reported to top management.

The Audit Commission developed a useful set of questions to enable auditors and others to undertake spot checks to assess data quality: consider the following key questions when assessing the system:

- Does the system appear to be adequately designed to ensure the data is accurate, valid, reliable, timely, relevant and complete?
- Are there any issues which need to be addressed in the testing of the underlying data, for example are aspects of the data provided by a third party?
- Does the spot check need to take account of specific risks, for example, where system providers have changed?
- Do the samples to be tested need to be directed to particular aspects of the service or definition being measured, or the system used to collect and process the data?

Many councils have adopted such procedures to underpin reporting on the National Performance Indicators. Although the requirement to submit these to central government may well change under the Coalition Government's arrangements, the imperative for such procedures as part of good management practice remains. Councils will want to ensure its data is robust both for its own arrangements for decision making and review and also for accountability to the public.

### Case study

A number of good examples of a simple process for data assurance can be found on the Policy & Performance Community of Practice

(<http://www.communities.idea.gov.uk/c/12404/forum/thread.do?backlink=ref&id=8378173&themeld=992387> ).

These include: North Lincolnshire, St. Helen's, Harlow, Hampshire County and Nottinghamshire County councils.

Blackpool Borough Council's "Performance Indicator Data Quality Audit Checklist" is illustrated here. Among other items, it seeks to identify or clarify:

- definition used,
- officer responsible,
- written procedures,

Performance Indicator Data Quality Audit Checklist		
Name:		Date:
PI No:		PI Contact Details:
PI Description:		
<b>Definition</b>		
	<b>Result</b>	<b>Reference</b>
Has the correct definition been used in calculating the PI output?		
<b>Calculation</b>		
	<b>Results</b>	<b>Reference</b>
The responsible officer has obtained details of the relevant PI definition and all appropriate guidance (and applied appropriately)?		
Has a written procedure for data collection been developed?		
Is the version of the procedure current and in date?		
Does the written procedure accurately reflect all stages of data collection and calculation?		
Has the correct denominator and numerator been used?		
Is the arithmetic in the calculation correct?		
Have figures been transposed correctly from the working paper to the report PI?		
All working papers on the evidence files have been appropriately cross-referenced?		
The checklist & working papers detail the exact methodology used (i.e. which systems accessed, versions used, reports run etc. - details or attachments of these are related with the checklist or on a separate computer file)?		
The checklist has been fully completed by the responsible officer?		
The checklist & working papers provide details on how the indicator value has been calculated?		
The completed checklist has been reviewed by a second officer?		
Are officers aware of the submission date?		
Do officers know who to submit data to both internally and externally?		

- methodology and working papers used checked,
- calculations correct and accurately transposed from system/working paper to report, and
- completed checklist reviewed by second officer.

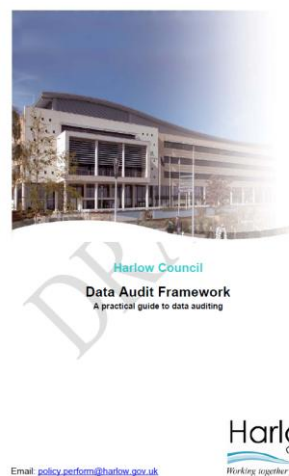
Where data is regularly used for decision making, the authority needs to put in place a system of internal control and validation. Key components for this include:

- Internal and external reporting requirements have been critically assessed. Data provision is reviewed regularly to ensure it is aligned to these needs.
- Data used for reporting to those charged with governance are also used for day-to-day management of the body's business. As a minimum, reported data, and the way it is used, are fed back to those who create the data in the first place, to reinforce understanding of their wider role and importance.
- Data is used appropriately to support the levels of reporting and decision making needed (for example, forecasting achievement, monitoring service delivery and outcomes, and identifying corrective actions). There should be evidence that management action is taken to address service delivery issues identified by reporting.
- Data used for external reporting should be subject to rigorous verification, and to senior management approval.
- All data returns are prepared and submitted on a timely basis, and are supported by a clear and complete audit trail.

### Case study

Harlow District Council has published a Data Audit Framework. Its data auditing process measures how fit for purpose an authority's data is. It involves profiling the data and assessing the impact that poor quality data has on the organisation's performance. The Framework provides specific guidance on how to plan and execute a data audit and covers the following areas:

- 1.0 Introduction to data auditing
  - 1.1 Our aims for data auditing
  - 1.2 The Need for a Data Audit Framework
  - 1.3 How the Data Audit helps
  - 1.4 The Data Audit Checklist
- 2.0 Guidance for using the Data Audit Framework
  - 2.1 Identifying and classifying the data
  - 2.2 Planning the Audit
  - 2.3 Assessing the management of the data
  - 2.4 Reporting findings and recommending change
- 3.0 Roles and Responsibilities
  - 3.1 The Performance Link Officer
  - 3.2 The Data Owner
  - 3.3 Policy and Performance
- 4.0 Frequently Asked Questions



## Accessing data - record naming conventions

A naming convention aims to foster a shared approach in an organisation to the titles of essential files, folders, documents and records. These are items which are essential to the operation of the business or which need to be retained for legal purposes. It is relevant to data quality policy as data will be collected and retained in files, folders and other records. Anyone with an interest in accessing such information (service users, managers, auditors etc.) needs to be clear about where to find key data; hence the desirability of a common approach. Such a convention applies to both paper based and electronically stored data and information.

A naming convention allows:

- Better access to records, files etc.
- Sorts documents into an easily understood system



- Allows for better management of records so that decisions on retention or disposal of files can be easily made

Typically, a naming convention might cover:

- Subject name
- Type of record (report, strategy, agenda, minutes, accounts)
- Origin (e.g. organisation, department, author)
- Applicable date (either specific date of event, or period document covers, e.g. Strategy 2010-14)
- Status (e.g. draft/final, version number)

### Case studies

Nexus (the Tyne & Wear Passenger Transport Executive) adopted their guidance “How to name your records” in October 2008. This can be downloaded from the Data Quality Community of Practice – library items (<http://www.communities.idea.gov.uk/c/79131/d/oclib/unthemed-index.do> )

Stirling Council use a spreadsheet to set out the key features of their file and record naming conventions. This is also accessible from the Data Quality Community of Practice.

#### How to name your records: Saving a file or record

All documents must adhere to the following naming structure

[prefix code][control no.] – document name[version]\_[date]



Field	Description	Format
Prefix Code	Unique departmental code	2 or 3 upper case characters
Control No	Unique reference number	3 to 6 digits
Document Name	Users own description of the document – this is NOT the users name	Max 50 characters not to include non-descriptive words
Date	The date which the document was saved	YYMMDD (reverse order)

#### Version and Draft Controls

When saving or resaving a document a 'version number' must be included after the 'Document Name', to indicate whether the amendment made to the document is a minor update or a major update.

A **minor** update would be indicated by the version number changing to one decimal place e.g. 1.1, 1.2, 1.3 etc.

A **major** update would be indicated by the version number changing as a whole number e.g. 1.0, 2.0, 3.0 etc.

Any document with a version of less than 1 (e.g. v0.12) denotes a draft document.

Return to [Table of Contents](#)

## Data sharing

### Data sharing and partnership working

Sharing relevant data between services and with partner organisations is vital if we are to address the complex needs of those dependent on public services. But it needs to be balanced with protecting individual privacy and keeping within legislation. Data sharing must comply with Article 8 of the Human Rights Act 1998 (“Everyone has a right to respect for his/her private and family life, his/her home and his/her correspondence”), subject to exemptions relating, for instance, to public safety and protection of individual rights and freedoms.

Data sharing can make a major contribution to tackling many of the difficult issues facing public services particularly where service users are clients of multiple services such as children at risk, vulnerable adults and the recently bereaved. Data shared between departments and partners can make a major impact on

- planning, commissioning and targeting services
- tailoring what is provided to the needs of individuals, households and communities
- identifying where people and localities might be particularly subject to danger or risk of harm

Many of the high profile failures in local public services have been directly or indirectly due to the failure to share critical data, such as:

- The Soham murders. One of the key failings was the inability of Humberside Police and Social Services to identify the behaviour pattern of the man found guilty of the murders, Huntley, remotely soon enough. That was because both viewed each case in isolation and because Social Services failed to share information effectively with the police. It was also because, as the Humberside Chief Constable admitted in his evidence, there were “systemic and corporate” failures in the way in which Humberside Police managed their intelligence systems.’ (*The Bichard Inquiry 2004*)

- The Baby Peter and other child abuse cases. Public inquiries and case reviews of such cases invariably point to the lack of shared data as a critical reason for the failures resulting in death or serious injury to children at risk.
- The Pilkington case. The death of Fiona Pilkington, who killed herself and her disabled daughter after years of abuse from a gang in Barwell, Leicestershire, again identified that data and information had been available but not shared adequately, leading to a subsequent joint effort by the police and social care services to identify people who may be vulnerable to anti-social behaviour.

In 2007, the Government commissioned Richard Thomas, the Information Commissioner, and Dr Mark Walport, the Director of the Wellcome Trust to consider a range of issues around data sharing.

Among the Thomas/Walport recommendations were:

- As a matter of good practice, all organisations handling or sharing significant amounts of personal information should clarify in their corporate governance arrangements where ownership and accountability lie for the handling of personal information.
- Public bodies should publish and maintain details of their data-sharing practices and schemes, and should record their commitment to do this within the publication schemes that they are required to publish under the Freedom of Information Act.
- Government departments and others wishing to develop, share and hold data-sets for research and statistical purposes should work with academic and other partners to set up safe havens.

The report put forward some simple ground rules to aid sound decision making about sharing personal information:

- Organisations must have effective controls in place, setting out clear lines of accountability and aiming for maximum transparency, to safeguard the personal information they hold and share.
- In line with the principle of minimising the amount of data collected and used, organisations should collect and share only as much personal information as is essential and store it only for as long as is necessary.
- Organisations must train their staff to understand the risks of handling personal information and to meet the reasonable expectations of those whose data they hold, and of the regulator.
- Whether or not personal information should be shared can be considered only on a case-by-case basis, weighing the benefits against the risks.
- The case for sharing personal information will usually be stronger when it brings clear benefits, or when not sharing personal information may risk significant harm.
- The sharing of personal information should be adequately documented and subject normally to privacy impact assessments.
- When organisations share personal information, they must pay particular attention to these inherent risks: perpetuating or exaggerating inaccurate or outdated data; mismatching data; losing data; and intruding excessively into private lives. This becomes even more critical when entire databases are shared.

As an illustration of how easily the benefits of data sharing can be blunted, the Home Office published, in December 2010, an evaluation of an initiative to encourage data sharing between hospitals accident & emergency units and local community safety partnerships (CSPs) in the South East.

*The report found that “Two common concerns were identified by interviewees in relation to the quality of the data collected on assault victims. First, staff in most areas did not believe their scheme had been successful in capturing the total number of assault patients passing through the Hospital Emergency Department. Second, in terms of the quality of information collected on individual assault patients, location of the assault was often perceived to be poorly recorded.”*

*The report also found that “The impact of high staff turnover amongst those collecting the data (particularly among non-receptionist staff), and wider issues of motivation*



*were also cited as factors inhibiting the quality of data collection. Interviewees did, however, identify a range of approaches to improve the quality of data collection through focusing on the motivation and commitment of data collection staff. These included: encouraging two-way feedback between data collectors and data users; training sessions; raising and maintaining awareness of the scheme; and working to improve motivation of staff."*

In other words, the factors limiting the effectiveness of sharing good quality data between public agencies were the same as those affecting the performance of individual authorities. As councils and their partners increasingly focus on local outcomes, they will inevitably have to consider how best to reconcile different systems for recording activity and for sharing data on shared objectives, policies, plans and programmes. The sharing of data raises major issues of trust as well, in certain circumstances, of legal responsibilities.

### **Case studies**

#### **A partnership approach to sharing information and improving services in Swindon**

Swindon Council worked with local partners and the third sector to develop a new homelessness strategy and new services for the area. The Council commissioned an independent review of how homeless people viewed and used the full range of local services. The results of the review were combined with existing data and analysis from the Council and partners including the police, the primary care trust and the local anti-social behaviour unit. The Council used the findings from the data, analysis and the review to set up a multi-agency steering group to plan for a new homeless day centre in Swindon.

#### **Sharing information to understand and set local priorities in Somerset**

The Council analysed and triangulated a range of data with consultation data to ensure it understood local needs and issues. Sharing data in this way identified issues the Council had not previously understood or prioritised, including understanding the complexity of problems such as fuel poverty, domestic violence and road traffic accidents. The process also highlighted the danger of making assumptions. Somerset was above average on most measures, but this can mask the position in some localities.

*"Before, there was a tendency for everyone to say x ward is deprived so they will have all the problems. But when we really looked at the data it didn't always follow."* (the Somerset Local Area Agreement Manager)

For example, on fuel poverty a village called Bishops Lydeard has some of the worst fuel poverty in Somerset. This was due to an antiquated gas system combined with shoddily built post war housing. This had not been picked up before. *"With domestic abuse, we thought it was worse in deprived wards – but domestic violence is no respecter of traditional expectations. And when we dug deeper, the falls data was a surprise to us as was the numbers of people killed and seriously injured in road traffic accidents."*

*These examples were highlighted in the Audit Commission's study ["Is there something I should know?"](#)*

### **Data sharing and geographical information systems**

Data sharing at an address level is very easy to achieve via geographical information systems (GIS). The value of plotting data from different services and agencies is illustrated in the case study of Leicestershire Police and Adult Social Care services mentioned above (The Fiona Pilkington case) When commissioning new systems, councils and other partners need to consider how such systems can share data with other systems used in other parts of the organisation or partnership.

## *Data sharing for benchmarking*

The Local Authority Performance Solution (LAPS) is a pioneering project to share, compare and analyse local performance data collected by London boroughs to improve services for all Londoners. The project is led by Capital Ambition (the Improvement & Efficiency Partnership for London) and the London borough of Lewisham. London boroughs have agreed to regularly share and analyse this data on a capital-wide basis, allowing them to compare their own performance with others and, by factoring in the cost of services as well as outcomes, to accurately assess their relative value for money. With data provided quarterly, LAPS delivers timely analysis that enables an early identification of areas where innovations or best practice are performing well and delivering value for money – helping drive up performance for all boroughs. By working together to share this data London boroughs are developing an open and transparent means of assessing the comparative costs, performance and value of public services across the capital. Forthcoming enhancements will include enabling boroughs with similar demographic and social profiles to compare their relative performance on a service by service basis. Importantly, following the coalition government's decision to change the national performance and inspection regime for local services, work has begun on reviewing the key measures of performance that London would wish to use in an era of greater devolution.

## *Data sharing protocols*

It is good practise to publish a set of ground rules or principles to be followed by all services and partner agencies who provide or receive data. Effective data sharing needs to foster mutual trust in the exchange of information between individuals and organisations. This of course applies across service departments within councils as well as with partner agencies. The following principles are suggested as a starting point for such an agreement:

- Data should be easily accessible
- When data is supplied, accompanying information on its ownership, methods and scale of collection and limitations of interpretation, should be provided.
- A clear statement of authority should be made when data is shared with others, to ensure recipients respect any associated intellectual property rights and copyright law regarding their duplication and use. This is to reduce potential problems when data is made available, so that those supplying and those managing data on other people's behalf can do so with confidence.
- Recipients of data should make clear how, when and where they will use this data, so that data providers have confidence that control will be exercised in its management and use. This aims to encourage trust and transparency between those who have supplied records and those who might be managing data.
- Personal data must be managed in accordance with the principles of the Data Protection Act 1998 and any successor legislation.
- Data should be made available at no cost

Some authorities have developed such arrangements including councils, police, health and fire & rescue authorities in Hampshire:

### **Case study**

The various organisations making up the Hampshire local strategic partnerships (the “Hampshire Senate”) agreed, in 2008, a data sharing & quality protocol. Its purpose is to:

- facilitate the sharing of good quality data between agencies, groups and individuals...
- help partners get the most value from data by communicating the partnership’s commitment to data quality and improving the quality of data so that it is accurate, valid, reliable, timely, relevant and comprehensive.
- give the necessary assurance to those using information to make decisions, assessment or judgements

Partners agree to co-operate with each other and to fully and properly use its principles, procedures and supporting forms. The types of data include non-personal and personal data (subject to the provisions of the Data Protection Act) and “de-personalised” data. The protocol is intended to provide a consistent framework and common standards for different partner organisations in Hampshire to adopt. By accepting the protocol, an organisation expresses its desire to share quality information in a lawful and controlled way.

Return to [Table of Contents](#)

## **Data protection – myths and realities**

The Data Protection Act 1998 seeks to strike a balance between individual concerns and the common good, giving individuals certain rights of privacy regarding information held about them and placing obligations on those who process information.

The aim of the Data Protection legislation is that “all organisations should inspire trust by collecting and using personal information responsibly, securely and fairly” (Richard Thomas, Information Commissioner). It should not be used as an excuse not to share important information between organisations where the public might otherwise be put at risk (see, for example, the inquiry into the Soham murders highlighted above).

### ***Data Protection Act 1998 – underlying principles***

Personal information must be:

- *Fairly and lawfully processed*
- *Processed for limited purposes*
- *Adequate, relevant and not excessive*
- *Accurate*
- *Not kept longer than necessary*
- *Processed in accordance with citizen rights*
- *Secure*
- *Not transferred to other countries without adequate protection.*

In practice, these mean:

- Data may only be used for the specific purposes for which it was collected.
- Data must not be disclosed to other parties without the consent of the individual whom it is about, unless there is legislation or other overriding legitimate reason to share the information (for example, the prevention or detection of crime). It is an offence for other parties to obtain this personal data without authorisation.

- Individuals have a right of access to the information held about them, subject to certain exceptions (for example, information held for the prevention or detection of crime).
- Personal information may be kept for no longer than is necessary and must be kept up to date.
- Personal information may not be sent outside the European Economic Area unless the individual whom it is about has consented or adequate protection is in place.
- Subject to some exceptions for organisations that only do very simple processing, all entities that process personal information must register with the Information Commissioner's Office.
- Entities holding personal information are required to have adequate security measures in place. Those include technical measures (such as firewalls) and organisational measures (such as staff training).
- Subjects have the right to have factually incorrect information corrected

The Government's Ministry of Justice issued a call for evidence in summer 2010 and an impact assessment on current data protection law to help inform the UK's position on negotiations for a new EU data protection instrument, expected to start in early 2011.

### **Data handling – the risk of misplaced or lost records**

Following the high profile loss of data by HM Revenue and Customs and other public bodies, public confidence in the Government's, and the wider public sector's, ability to securely protect its information is at an all time low. Councils also need to restore public confidence that they will protect their privacy and use and handle their information professionally.

In June 2008, the Cabinet Secretary published 'Data Handling Procedures in Government'. This guidance focused on central government bodies but recognises the crucial role of local councils. Thus the Local Government Association (LGA) and the Welsh Local Government Association (WLGA) agreed to produce equivalent standards for local government.

This considers how data can be kept safe and how it should be handled. The standards are structured around four themes:

1. **People** – All councils should seek to develop a culture that properly values, protects and uses information for the public good. Councils should reinforce that information is a key business asset and that its proper use is not simply an IT issue. There should be clear lines of accountability throughout the organisation together with a programme of staff awareness raising, starting at induction but continually updated, which clearly sets out the expectations of staff.
2. **Places** – All councils should ensure the security of their information through the physical security of their buildings, premises and systems. There should be regular assessments of information risks, which are discussed by senior management.
3. **Processes** – All councils should check that they have proper document systems in place and that their suppliers and contractors, when handling their information, work to the same standards. Councils should also monitor and audit the effectiveness of their policies and, where appropriate, engage independent experts to test ICT systems and make recommendations.
4. **Procedures** – All councils should produce a Corporate Information Risk Policy which sets out how they will implement the measures in this document, as well as produce policies for risk reporting and risk recovery. They should ensure that there are mechanisms in place to test, monitor and audit the policies and procedures of the council.

*From: Local Government Data Handling Guidelines LGA & WLGA, Nov 2008*

The Society for Information Technology Managers in local government (Socitm) has produced a simple "Top 10 tips" for Data Handling:

1. Ensure you understand which legislation affects your service area.
2. Ensure a named individual in the service unit or department (not ICT) takes responsibility and owns the risk.
3. Ensure there is an effective incident reporting mechanism in place.
4. Regularly monitor, measure and audit your processes and procedures.
5. Establish a Corporate Information Governance group.

6. Ensure all staff are trained, updated and aware of their responsibilities.
7. Undertake regular risk reviews of all processes and procedures.
8. Ensure all key information assets are classified and are resilient.
9. Have robust risk driven processes in place for “ad hoc” situations.
10. Have documented policy driven processes and procedures in place.

Return to [Table of Contents](#)

## Data security – the risk of unlawful or malicious attack

Closely related to the risk of misplaced or lost records, is that securing sensitive data from unlawful or malicious attack. A quarter of all councils had suffered a security breach in the year 2009-10 and in half these cases, the impact was felt at board level, according to a survey conducted by the Local Government Chronicle.

Among the cases of risky practices which have been publicised in recent years are:

- information sent, unsecured, through the internet rather than secure channels
- Use of internet cafes and laptops in open areas when handling sensitive information
- Use of webmail to store confidential information
- Unencrypted data stored on disks, memory sticks and other portable storage devices – all vulnerable to theft or being mislaid
- Confidential waste discarded without adequate destruction or shredding

The survey (reported in the LGC, 22 April 2010) showed that 86% of councils provided staff with guidance on the Data Protection Act and Freedom of Information Act and that 81% of councils have adopted a security policy that is “widely available” to staff. However, less than 20% made data security a board-level responsibility and a third allocated responsibility to an IT officer (see SOCITM’s recommendation no. 2 above). Also, only a third of councils trained board members on risks associated with data security and a similar number claimed they regularly updated staff on new security practices.

## The future?

There is a real danger that the recent focus on the quality of local authority data will, in future, decline. The likely reduction in demand by central government for data on local performance, coupled with less inspection and external review of council’s systems and procedures may divert attention elsewhere.

However, the better managed authorities will continue place an emphasis on ensuring the data they need for their own decision making and for external accountability remains of high quality.

It is hoped that this Toolkit will provide a ready source of reference to support such practices. However, as circumstances change, it is inevitable that new thinking and approaches will emerge. Ideally, this document will itself be used as an open source of material, attracting updates, corrections and new insights from practitioners. To help potential contributors, a version of this toolkit has been placed on the Local Government Improvement & Development’s “Managing Local Performance” wiki site (<http://ideamp.wetpaint.com/page/Data+%26+Data+Quality> ). All interested in this important topic are recommended to assist in keeping this material refreshed.

In the meantime, the author commends the various forums and communities of practice to ensure the drive for high quality data underpins all aspects of our public services.

## Kevin Ambrose

*For the Strategy Unit, Local Government Improvement & Development*

Last updated: 9<sup>th</sup> December 2010

## Further Information

### Publications

- *Nothing but the truth?* (Audit Commission, Discussion Paper, November 2009)
- *Is there something I should know? Making the most of your information to improve services* (Audit Commission, Local Government National Report + Self assessment framework, July 2009)
- *Data quality management in local authorities* (Capital Ambition *Data Connects* project in association with Tribal Group, June 2009)
- *Local Government Data Handling Guidelines* LGA & WLGA, Nov 2008
- *In the know: Using information to make better decisions* (Audit Commission, Discussion Paper, February 2008)
- *Improving Information to Support Decision Making: Standards for Better Quality Data*, (Audit Commission, 2007)
- *A Manager's Guide to Performance Management* (Audit Commission and Improvement and Development Agency for Local Government, 2006).
- *Figures You Can Trust: A Briefing on Data Quality in the NHS*, (Audit Commission, 2009)
- *Data Quality Management: At the Core of Managing Risk and Improving Corporate Performance* (PricewaterhouseCoopers, 2004).
- *Managing the Quality of Official Statistics* (Statistics Commission, Report No. 27, 2005).
- *Joint Area Review of Haringey Children's Services Authority Area*, (Ofsted, Healthcare Commission and HM Inspectorate of Constabulary, 2008)
- *Safeguarding Adults*, (Commission for Social Care Inspection, November 2008)
- *Process evaluation of data sharing between Emergency Departments and Community Safety Partnerships in the South East* (Home Office Research Report 46, December 2010)

### Web

- Data Quality Community of Practice  
<http://www.communities.idea.gov.uk/c/79131/home.do>
- Data Connects Forum (for London councils):  
<http://www.londoncouncils.gov.uk/capitalambition/projects/dataconnects.htm>
- Data.gov.uk: <http://www.data.gov.uk/>

## Acknowledgements

The author would particularly like to acknowledge the contributions of the following and their permission to use material from their organisations:

Natalie Penrose	Audit Commission
Robin Raily	Bolsover District Council
Jon Swift	Suffolk County Council
Tony Ellis	Brent Council
Michelle Parfitt	Gravesham Borough Council
Bruce Hill	Tonbridge & Malling Borough Council
Ruth Grimshaw	Blackpool Borough Council
Katrina Barnard,	Harlow District Council
Edd Smith	Nexus (Tyne & Wear PTE)
Sue Sylvester	Hampshire County Council

Return to [Table of Contents](#)