Public sector

May 2006

audit commission

Code of Data Matching Practice 2006

Audit Commission National Fraud initiative

The Audit Commission is an independent body responsible for ensuring that public money is spent economically, efficiently and effectively, to achieve high-quality local services for the public. Our remit covers around 11,000 bodies in England, which between them spend more than £180 billion of public money each year. Our work covers local government, health, housing, community safety and fire and rescue services.

As an independent watchdog, we provide important information on the quality of public services. As a driving force for improvement in those services, we provide practical recommendations and spread best practice. As an independent auditor, we ensure that public services are good value for money and that public money is properly spent.

For further information about the Audit Commission, visit our website at www.audit-commission.gov.uk

For additional copies of Audit Commission reports please contact:
Audit Commission Publications, PO Box 99, Wetherby LS23 75A Tel: 0800 502030

First published in May 2006 by the Audit Commission for local authorities and the National Health Service in England, 1st Floor, Millbank Tower, Millbank, London SW1P 4HQ

ISBN xxxx

Foreword by the Audit Commission

Over the last decade the National Fraud Initiative (NFI) has successfully detected fraud and overpayments totalling almost £300 million. This has enabled public money to be redirected back towards the public services for which it was always intended. Active detection and prosecution of fraudsters is a vital deterrent to others contemplating defrauding the public purse.

In addition to bringing these benefits, the data matching exercises are an efficient tool for assisting auditors to make their statutory assessment of the financial control and value for money arrangements put in place by audited bodies. Further, as a consequence of investigating matches that reveal overpayments, underpayments and other inaccuracies in records, the accounts of audited bodies will be corrected.

The Audit Commission encourages all those participating in the NFI, both auditors and bodies supplying data for matching, to comply with both best practice and the law when sharing and matching personal data. To that end, the Commission has issued this Code, which updates its first Code of Data Matching Practice published in 1997. This revised Code reflects changes in the law since 1997, and improvements and modifications to the NFI in light of experience drawn from four national exercises.

The Code sets out the principles and practices that should be adopted to ensure appropriate safeguards are built into the NFI. The matching process must be proportionate so that fraud is prevented and detected, whilst law-abiding citizens' privacy and rights are respected and protected. A key aspect of the Code is to provide good practice examples of how individuals should be informed of the checks carried out.

This Code applies in relation to the statutory audit of bodies in England to which the Audit Commission appoints auditors. Similarly successful data matching exercises undertaken in Wales, Scotland and Northern Ireland, with the assistance of the Audit Commission, will be subject to separate Codes.

NFI is a very successful example of joined-up working between the various organisations involved. The Audit Commission will continue to develop the initiative, identifying new areas where data matching can be used to detect and deter fraud against public bodies.

Sir Michael Lyons, Acting Chairman

Foreword by the Information Commissioner

Safeguarding public funds from those who seek to make fraudulent claims engages significant public interest concerns. Past evidence produced by the Audit Commission indicates the success of deploying data matching techniques in identifying fraud and preventing overpayments. However, data matching activities involve bringing together and cross comparing extensive amounts of personal information often drawn from a wide range of sources sometimes completely unconnected with the actual payment of the benefit claimed. Given that most of the information drawn together is about people who are not subsequently identified as being involved in benefit fraud, the use of powerful data matching techniques raise substantial data protection and privacy concerns. It is important that these are addressed and I welcome the Commission's Code of Data Matching Practice as it recognises the need to address these significant concerns and sets out important safeguards to ensure that National Fraud Initiative data matching activities take place in accordance with the requirements of the law.

The true test of any Code of Practice is measured by whether it is followed by those at which it is aimed. I particularly welcome the invitation by the Commission to review its processes during all data matching exercises and the encouragement given to Supplying Bodies to extend to me a similar invitation to review their procedures. I encourage those affected to pay close attention to the Code's provisions and adhere to them. The provisions not only help ensure compliance with the law but also help inspire public confidence that potentially intrusive activities are undertaken in a proportionate way with due respect for legitimate privacy concerns. Compliance with the Code should help ensure that those who are involved in fraudulent activities continue to be identified and held to account and the majority who are not are protected from unwarranted intrusion into their private lives.

Richard Thomas, Information Commissioner

1

Introduction to the Code

1.1 The Audit Commission

1.1.1 The Audit Commission ('the Commission') is responsible for appointing auditors to local government and National Health Service bodies ('audited bodies') in England. The Audit Commission Act 1998 ('ACA 1998') requires the Commission to appoint auditors to each audited body.

1.2 Appointed auditors for the purpose of the National Fraud Initiative

1.2.1 To minimise costs, the Commission has approved an arrangement under section 3(9) of the ACA 1998 whereby one auditor undertakes a comprehensive national data matching exercise on behalf of all appointed auditors. All appointed auditors may be involved in the review of audited bodies' arrangements for investigating matches and acting upon instances of fraud and identified weaknesses in internal controls.

1.3 Background to the National Fraud Initiative

1.3.1 It is vital that public bodies have adequate controls in place to prevent and detect fraud and error. The prevention and detection of fraud in local government and the health service is a major concern of those bodies as well as the Commission and its appointed auditors. Data matching exercises assist auditors in their assessment of the arrangements that have been put in place by audited bodies and assist audited bodies to identify fraud and error.

1.3.2 In 1996, the Commission launched a national fraud initiative, the NFI, to study the extent to which the benefits from a successful data matching exercise, based on local authorities in London, were applicable nationally. The Commission decided in 1998 that the NFI should form a regular part of the statutory audit, conducted at such intervals as the appointed auditor considered necessary.

1.3.3 Data matching involves comparing the extent to which computer records held by one body match against other records held by the same or another body. Computerised data matching techniques are used by the appointed auditor to narrow down the search for duplicate or fraudulent claims made upon audited bodies. A supplying body receives a report identifying instances of matching data within that body's own records and between that body's records and those of other relevant bodies. It is for the supplying body itself to

investigate the matches, so as to detect instances of fraud, over or underpayments and other errors and to update its records accordingly.

1.3.4 NFI in 1998 detected fraud and overpayments to the value of £42 million, details of which were reported in *A Perfect Match* (published in May 2000). NFI in 2000 detected fraud and overpayments in excess of £50 million, details of which were reported in *Match Winner* (published in May 2002). The exercise completed in 2002/03 was the subject of a national report in May 2004 and this revealed fraud and overpayments of £83 million. The latest exercise in 2004/05 has detected £107 million (national report published in May 2006). This brings the total detected fraud and overpayments to date (including pre-1998 exercises) to £300 million.

1.4 Purpose of the Code

1.4.1 The Commission is concerned:

- to ensure that its officers, its appointed auditors and all bodies involved in data matching conduct or participate in the NFI in a manner which complies with the provisions of the Data Protection Act 1998 ('DPA 1998') and the general law; and
- to ensure that all involved in the NFI follow good practice.

1.4.2 To assist in these objectives, the Commission has drawn up this Code of Data Matching Practice.

1.5 Status and force of the Code

1.5.1 All bodies required by the auditor to supply personal data for the purpose of the NFI should comply with the provisions of this Code. This is to ensure that the NFI is conducted in a manner which meets with the requirements of the DPA 1998 and the general law and achieves good practice. It should be noted that the DPA 1998 provides for certain exemptions from some of its provisions, and the extent to which these exemptions will apply are set out in the Code.

1.5.2 Where an appointed auditor becomes aware that a body has not complied with the requirements of the Code, the auditor will notify the body concerned and seek to ensure that it puts in place adequate measures to meet the Code's requirements.

1.5.3 Bodies which participate or propose to participate in the NFI may reproduce the text of this Code as necessary to facilitate the participation of their organisation in the exercise and to ensure all personnel involved are aware of their obligations under the Code.

1.6 Structure of the Code

1.6.1 The Code comprises:

- an explanation of the status of the Code and definitions of key terms used in the Code;
- principles governing data matching exercises;
- practical steps to be adopted by the Commission, its auditors and Supplying bodies to comply with those principles;
- an explanation of how compliance with the Code will be monitored, within the Commission and in relation to Supplying bodies;
- specific requirements, including good practice letters to data subjects and example declarations for supplying body documentation; and
- relevant provisions from the Codes of Audit Practice and statute law at Appendices 2-4.

1.7 Adoption and review of the Code

1.7.1 The 2006 Code will take effect from 20 April 2006, the date on which the Audit Commission approved it, following the conclusion of a formal consultation process. The 2006 Code will govern all future data matching exercises, until such time as it is reissued.

1.7.2 The Commission intends to review and update the Code periodically in the light of changes in the law and to reflect users' comments and experience drawn from each data matching exercise.

1.7.3 In addition, the Information Commissioner has been invited to review the Commission's processes during all data matching exercises, and wishes to be invited by Supplying bodies to review their procedures. The purpose of this review would be to monitor compliance with data protection principles.

1.8 Queries about the Code

1.8.1 Any questions about this Code, about NFI generally or about a particular data matching exercise should be addressed to Peter Yetzes, Associate Director, Audit Commission, 1st Floor, Millbank Tower, Millbank, London SW1P 4HQ; tel 020 7166 2222; email nfiqueries@audit-commission.gov.uk

2

The Code of Data Matching Practice

2.1 Status and scope

2.1.1 All bodies supplying data for data matching should observe the provisions of this Code. A copy of the Code will be issued to each Supplying body and to the Commission's appointed Auditors. It will also be published on the Commission's website.

2.1.2 The Code will be observed by the Commission and its appointed Auditors when undertaking data matching exercises.

2.1.3 The Information Commissioner regards the provisions of the Code as setting good practice standards that will help organisations to comply with data protection principles.

2.1.4 This Code is not intended to apply to any steps taken by a supplying body to follow up or investigate matches arising from the NFI.

2.1.5 This Code applies for the purpose of the statutory audit of audited bodies in England.

2.2 Definitions

2.2.1 For the purposes of this Code the following definitions apply:

'Auditor' is an auditor appointed by the Audit Commission under section 3 of the Audit Commission Act 1998 ('ACA 1998') to an audited body, or a person approved by the Audit Commission under an arrangement under subsection (9) of that section;

'Audited body' is a local government or NHS body to which the Commission appoints an external Auditor. This includes police authorities, local probation boards and fire and rescue authorities as well as local councils. These bodies are listed in Schedule 2 to the ACA 1998;

'Data matching' means the electronic comparison of two or more sets of personal data which have been collected for separate purposes in order to identify any information which is inconsistent for further investigation;

'Non-audited body' is a body other than one listed in Schedule 2 to the ACA 1998 but which supplies data to an Auditor. Auditors have power to call for data from non-audited bodies under section 6 of the ACA 1998 where they relate to a body subject to audit;

'Output' is the computer data file of reported matches in whatever format (but usually provided in the form of a CD-ROM) resulting from processing the data;

'Senior Responsible Officer' is the Director of Finance or other senior named officer of the Supplying body responsible for ensuring compliance with this Code;

'Supplying body' is either an audited or non-audited body which supplies data to an Auditor for the purposes of a data matching exercise;

The terms 'data', 'personal data', 'data subject', 'data controller' and 'processing' all have the same meaning as in the Data Protection Act 1998 ('DPA 1998').

2.3 Principles governing data matching exercises

2.3.1 To assist in complying with the DPA 1998 and the general law the following principles will be observed when undertaking data matching (further details of the practices required of the Commission, its Auditors and Supplying bodies to comply with these principles are detailed in section 2.4 below):

(a) Participation in data matching exercises carried out as part of the statutory audit is mandatory for:

- all audited bodies listed in Schedule 2 to the ACA 1998, except where an exemption is given; and
- all other bodies for whom an Auditor determines that their data relates to an audited body, and is required for NFI purposes.

(b) Data will be required by the Auditor from all bodies set out in (a) above under section 6 of the ACA 1998.

(c) New areas of data matching will be undertaken on a pilot basis to test the effectiveness of applying data matching to certain data sets. Only where pilots achieve matches that demonstrate a significant level of potential fraud will they be extended nationally in NFI. The terms of this Code will apply in full to pilot exercises taking place within NFI.

(d) Personal data shall only be obtained and processed in accordance with the DPA 1998.

(e) Supplying bodies must inform data subjects that their data may be disclosed for the purposes of auditing in order to identify possible cases of fraud.

(f) Wherever practicable the information required in (e) shall be provided prior to the initial collection of data from data subjects. It should in any event be provided prior to disclosure of the data to the Auditor unless it is impractical to do so.

(g) The disclosure of personal data by Supplying bodies to the Auditor as part of the data matching exercises is for the purpose of identifying possible cases of fraud and consequential correction of any under or overpayments detected.

(h) To ensure fair processing of data, the software, techniques and algorithms used in the data matching exercises are those which are indicative of potential fraud and/or under or overpayments only, and will be refined in the light of practical experience.

(i) No assumption should be made that matches are fraudulent. Auditors and audited bodies should review Output to eliminate coincidental matches, and concentrate on potentially fraudulent cases. In order to do so they will need to identify and correct those cases where errors have occurred.

(j) The data provided by Supplying bodies should be the minimum required to undertake the matching exercise and report the results. This will be set out in a handbook. The relevant handbook will prescribe the data that is sufficiently adequate and relevant (but not excessive) to enable individuals to be accurately identified during the data matching process and from the data matching Output, so as to give confidence in the data matching process.

(k) Data supplied by Supplying bodies must be of a good quality in terms of accuracy and completeness. Prior to supplying data for matching, bodies must ensure that the personal data are as accurate and up to date as possible.

(l) Data should be destroyed promptly once no longer required, unless needed by Supplying bodies as working papers for the purposes of audit, or for the purpose of continuing investigations or prosecution.

(m) Data should not be disclosed in the course of data matching exercises to parties beyond the defined scope of the NFI, unless there is specific legal authority for so doing.

(n) Security arrangements for handling and storage of data by all involved in the NFI should ensure that:

- specific responsibility has been allocated to one or more managers for security of data;
- security measures take appropriate account of the physical environment in which data is held, including the security of premises and storage facilities;
- there are logical controls to restrict access appropriately to electronic data; and
- all staff with access to data are given appropriate training.

2.4 Practical steps required to comply with the Data Matching Principles

2.4.1 The practices which should be adopted by the Commission, its Auditors and Supplying bodies to comply with these principles are summarised in the sections below, regarding:

- governance arrangements;
- requirements for fair collection and disclosure of personal data;
- data handling;
- intermediate processing;
- output control;
- access control; and
- data back-up.

2.5 Governance arrangements

2.5.1 The Director of Finance or equivalent senior named officer of each Supplying body will act as Senior Responsible Officer for NFI purposes. The Senior Responsible Officer will authorise named officers responsible for data handling, for follow up investigations and to act as key contacts with the Auditor, and will ensure they are suitably qualified and trained for their role.

2.5.2 For each data matching exercise, a handbook will be distributed to all Supplying bodies for that exercise, setting out the detailed requirements for participation in NFI. The most up-to-date handbook can be found on the Commission's website at www.audit-commission.gov.uk/nfi.

2.5.3 The handbook will contain:

- a list of the responsibilities of the nominated officers at the Supplying body;
- a Supplying body statistics return (requesting key facts and figures for each system to be matched);
- data specifications for each system (listing the minimum data to be provided by the supplying body to enable data matching and Output of sufficient quality);

- preferred data formats and media;
- a data checklist to be submitted with each dataset;
- a timetable for processing;
- a data protection compliance return; and
- an explanation of the significance of matches between particular data sets and the approach which should be taken in carrying out investigations.

2.5.4 Supplying bodies must have procedures in place for dealing appropriately with requests from data subjects for access to their data, and for complaints about the inclusion of their data in a data matching exercise. If requests for access to data are received during the matching exercise, requests that the Auditor is best placed to deal with should be passed on promptly so the Auditor can respond appropriately.

2.5.5 The Information Commissioner maintains a public register of data controllers. Each register entry includes the name and address of the data controller, and the purposes for which data is processed (identifying the data subjects and recipients for each purpose). It is the responsibility of all Supplying bodies to ensure their notification to the Information Commissioner includes Auditors as recipients against the appropriate purpose(s).

2.5.6 A Notification Handbook is available from the Information Commissioner, which sets out how to complete the required Notification Form. Notification templates are available from the Information Commissioner for local authorities, NHS and other public bodies. These include the disclosure of personal data to Auditors in certain circumstances. If these templates are not used by a Supplying body, the body must still ensure its register entry covers disclosures to appointed Auditors.

2.5.7 All Commission-appointed auditors are registered as data controllers for the purposes of NFI.

2.6 Requirements for fair collection and disclosure of personal data

2.6.1 **Collection of new data**. For data processing to be fair, the first data protection principle under the DPA 1998 requires data controllers to inform data subjects of the identity of the data controller, the purpose or purposes for which the data may be processed, and any further information which is necessary. Subject to certain

exemptions, which are described below, where practicable this should be done at the time of the original collection of the data from data subjects. Supplying bodies collecting new personal data that they know will be used for the purposes of NFI must inform data subjects at the point of data collection that their personal data may be disclosed for the purposes of auditing in order to identify possible cases of fraud.

2.6.2 Appendix 1 contains a standard fair collection notice for inclusion on benefit and other application forms. The notice covers the use of personal data in anti-fraud and data matching initiatives conducted both by the body collecting the data and by the Auditor. Data which have been collected on the basis of the recommended fair collection notice (or equivalent) may be disclosed to the Auditor for the purposes of the NFI.

2.6.3 **Use and disclosure of existing data**. Some of the data to be disclosed for the purposes of data matching may already have been collected without a fair collection notice having been provided at the time of the original data collection. In the case of the NFI, exemptions are available under the DPA 1998 from the requirement to provide fair collection notices at the time of the original data collection.

2.6.4 The principal exemptions on which NFI relies are under sections 29 and 35 DPA 1998. For those bodies in respect of which participation in data matching is mandatory, the exemption under section 35 DPA 1998 applies. The data from these bodies are required to be provided to the Auditor relying on powers under section 6 ACA 1998 (see principle (a) under 2.3.1 above). Section 35 exempts personal data from the non-disclosure provisions of the DPA 1998 where they are required under any enactment.

2.6.5 The exclusion of existing data from the exercise where fair collection notices were not provided at the time of the original collection is likely to prejudice the prevention or detection of crime, and to this extent the exemption in section 29 applies.

2.6.6 **Retrospective fair collection notices**. In the limited number of cases where it is not practicable to furnish data subjects with a fair collection notice at the time of the original collection of the data, retrospective fair collection notices should be given at the earliest reasonable opportunity to every individual data subject concerned (and in any event before disclosure to the Auditor) unless it is impracticable to do so. One example of when it might be impractical is where the current address is not known. Giving notice will enable all data subjects to know their data is being included in data matching and to take appropriate steps if they consider the use is unjustified or unlawful in their particular case.

2.6.7 **Considerations in different cases**. In the case of applications made by data subjects to the body concerned, a fair collection notice can be included in the application form intended for use by the data subject (see 2.6.2). Such notices will have the effect of deterring fraud as well as informing about the inclusion of the data in data matching.

2.6.8 In other cases (occupational pensioners, employees, tenants etc), Supplying bodies already communicate formally at least once a year in the form of a newsletter or payslip etc. Fair collection notices should be included in these communications, which should be sent to **named** individuals in advance of each NFI exercise, to ensure that all data subjects are advised. This will avoid the cost of a separate mailing. A number of Supplying bodies have already adopted this approach and a copy of a good practice example appears in this Code at Appendix 1.

2.6.9 In all cases communication with data subjects must be clear, prominent and timely.

2.6.10 The submission of data to the Auditor must be accompanied by a declaration from each body confirming compliance with the fair collection requirements set out in this Code. The Auditor will check that the requirements have been adhered to and, where necessary, will agree the steps necessary for the body to meet the Auditor's concerns.

2.6.11 **Deceased persons**. Some of the data used for data matching purposes in NFI relates to deceased persons. Although not classed as personal data under the DPA 1998, common law rules of confidentiality may restrict disclosure in certain circumstances. Particular care and sensitivity should be taken in dealing with data concerning deceased persons throughout the exercise, but particularly in the case of investigation of matches, to avoid any unnecessary distress and embarrassment.

2.7 Data provided by Supplying bodies

2.7.1 The data provided by Supplying bodies must be of good quality in terms of its accuracy and completion. Processing of inaccurate data could mean that the Supplying body is in breach of data protection and/or libel law. Before submission of data to the Auditor, errors identified from previous data matching exercises should be rectified, and action taken to address recommendations in data quality reports provided to the Supplying body. The Supplying body's key contact should check the readability of the data before despatch. This will help minimise the time that the Auditor retains the data.

2.7.2 Data provided by the Supplying bodies should be despatched to the Auditor by courier or special delivery.

2.7.3 All data in whatever form will be logged on receipt by the Auditor and stored securely in a fire-proof safe. All data stored electronically will be held on a secure, password-protected computer system maintained in a secure environment.

2.7.4 Data submitted as part of the NFI will not be passed to any third party (ie a person other than the bodies participating in NFI and the firm contracted to provide data matching services) by Auditors or their agents unless required by law.

2.7.5 All original data submitted to the Auditor in whatever form (tape cartridges, cassettes, diskettes, hardcopy and CD-ROMs) will be destroyed and rendered irrecoverable by the Auditor after all processing and re-runs are completed and all queries resolved. This will be done promptly and, in any event, within six months of the conclusion of the exercise.

2.8 Intermediate processing

2.8.1 The firm processing data on behalf of the Auditor will do so under a contract in writing which imposes requirements as to technical and organisational security standards so as to meet ISO 17799, and under which the firm may only act on instructions from the Auditor.

2.8.2 All intermediate data used in data matching exercises will be erased and rendered irrecoverable in the same timetable as original data (see 2.7.4 above).

2.9 Output control

2.9.1 All Output from data matching exercises (if on CD-ROM) should be distributed by courier or sent by special delivery to the Senior Responsible Officer (ie the Director of Finance or equivalent named senior officer of the Supplying body), together with a pack comprising: investigation guidelines, good practice protocols, Output overview, feedback forms and a list of key contacts. From 2006/07, distribution will be web-based, which should eliminate distribution logistical issues and strengthen access controls to data.

2.9.2 All Output from data matching exercises will be password protected and should be stored securely in a locked facility in a secure environment or on a secure, password-protected computer system as the case may be.

2.9.3 The circumstances surrounding an individual match will be considered by an investigator at the Supplying body before any decision is made consequent on that match. Investigating officers should refer to the investigation guidelines in the handbook.

2.9.4 Supplying bodies may retain the CD-ROM disclosed to them which contains data matches as working papers if required for the purposes of audit, or for the purpose of continuing investigations or prosecution. Supplying bodies should discuss with their Auditor what should be retained in their individual case, and subject to that, should ensure that data no longer required is destroyed promptly.

2.9.5 Auditors will review Output so that the data matching techniques and algorithms used can be refined for future exercises. Similarly, the data requirement specifications should be reviewed and refined.

2.9.6 No copies of any Output should be retained longer than necessary by the Auditor, except a single set of the 'match keys' in magnetic form, held securely offline by the Auditor. This is solely for the purpose of preventing duplication of matches in any subsequent data matching exercises.

2.10 Access control

2.10.1 All persons handling data as part of the data matching process should be made aware of their data protection and security obligations under the DPA 1998 and this Code and should be given appropriate training as necessary. Such staff should be subject to strict access authorisation procedures. Breach of authorisation procedures should attract appropriate disciplinary sanctions.

2.10.2 Access to data held in any form should only be granted to named individuals (Auditors, approved staff within the firm that undertakes the processing, or named officers of the Supplying bodies). The Senior Responsible Officer should ensure that each type of Output is disclosed only to appropriate officers by use of the installation menu provided for that purpose.

2.10.3 All computers used to process the data should have appropriate physical and logical access controls so as to limit access only to the named individuals. These controls should be subject to review by the Auditor.

2.10.4 File permission for all data files should be set so as to limit access at any level to the appropriate named individuals. Where a breach of security occurs, or is suspected, authorised users should be given new passwords or required to change their passwords as soon as possible.

2.11 Data back-up

2.11.1 All data submitted as part of NFI should be backed up by the Auditor at appropriate intervals, but not more often than is reasonably necessary. Back-ups will be subject to the same security, destruction and access controls as the original data.

3

Monitoring compliance with the Code of Data Matching Practice

3.1 Under section 51(7) of the DPA 1998 the Information Commissioner has been invited by the Commission to assess NFI compliance with the Act. To enable the Information Commissioner to do this it is also necessary to assess compliance of those bodies supplying personal data. For this reason all bodies supplying data for the purposes of NFI should accede to any reasonable request by the Information Commissioner to carry out an assessment of their processing of personal data. Such an assessment will be designed only to monitor compliance with the data protection principles.

Appendix 1

Specimen fair processing notes

Good practice example of notice to be included in application forms

(see paragraphs 2.6.1 and 2.6.7 of the Code)

'This authority is under a duty to protect the public funds it administers, and to this end may use the information you have provided on this form for the prevention and detection of fraud. It may also share this information with other bodies responsible for auditing or administering public funds for these purposes.'

Good practice example letter to data subjects

(see paragraph 2.6.8 of the Code)

This example has been drafted for pensioners; the words in [square brackets] should be amended accordingly for employees, tenants etc.

Dear {name [of pensioner]}

The {name of audited body} is under a duty to protect the public funds it administers. To this end from time to time it may use information provided to it for the prevention and detection of fraud and share it with other bodies responsible for auditing or administering public funds for these purposes.

The council is currently required to participate in an anti-fraud initiative operated by the Audit Commission's appointed auditors. For this initiative, we are providing details of [pensioners to the auditors so that they can compare these with information provided by other public bodies to ensure that no pensions are being paid to persons who are deceased or no longer entitled to them, and also with housing benefit records to ensure that occupational pension income is being declared.]

While the object of the exercise is the detection of fraud, previous exercises also uncovered underpayments [to pensioners], which were then rectified. These exercises, therefore, help ensure the best use of public funds.

Appendix 2

The Codes of Audit Practice

1 The Commission is required to prepare Codes of Audit Practice prescribing the way in which auditors are to carry out their functions under the ACA 1998. Codes of Audit Practice must be approved by a resolution of each House of Parliament at intervals of not more than five years. The current Codes were approved and published in 2005. They define the scope of auditors' responsibilities, of which some of the most relevant are set out in this appendix. The extracts are taken from the Code of Audit Practice for local government, but the equivalent sections of the Code of Audit Practice for National Health Service bodies are identical.

2 Data matching is an efficient audit technique which assists auditors in fulfilling their responsibilities, particularly in relation to the following provisions of the Codes of Audit Practice:

- The Codes require auditors to 'review and report on ... the audited body's financial statements and its statement on internal control; and whether the audited body has made proper arrangements for securing economy, efficiency and effectiveness in its use of resources.' Data matching results provide evidence to auditors of both frauds and under and overpayments, helping them to form a judgment as to whether the audited body has adequate arrangements in place.
- The Codes also require auditors to 'provide reasonable assurance that the financial statements are free from material misstatement, whether caused by fraud or other irregularity or error.' A significant number of over or underpayments identified using a data matching technique may give the auditor reason to believe that there has been a material misstatement of the accounts. This may in turn lead to audit recommendations to improve the systems of internal control in operation in the audited body.

Extracts from the Codes of Audit Practice 2005

(taken from the Local Government Code the NHS Code is virtually identical in relevant respects, though equivalent provisions may have different paragraph numbers.)

Scope of the audit and auditors' objectives

6 Because of the special accountabilities attached to public money and the conduct of public business, the scope of external audit in local government is extended to cover not only the audit of the financial statements but also the audited body's arrangements for securing economy, efficiency and effectiveness in its use of resources. The audit of the financial statements is covered by professional auditing standards and so this *Code* focuses more on how the wider range of functions of auditors appointed by the Commission should be carried out.

7 Auditors' objectives are to review and report on, to the extent required by the relevant legislation and the requirements of this *Code*:

(a) the audited body's financial statements and its statement on internal control; and

(b) whether the audited body has made proper arrangements for securing economy, efficiency and effectiveness in its use of resources.

The audit approach

10 Auditors should carry out the audit economically, efficiently and effectively, and in as timely a way as possible. In framing an audit approach to meet the objectives of the audit, they should:

(a) plan and perform the audit on the basis of their assessment of audit risks, determining where to direct their work and to allocate resources to ensure that the audit is tailored to the circumstances of the audited body. They should obtain such information and explanations as they consider necessary to provide themselves with sufficient evidence to meet their responsibilities under statute and the *Code*. Auditors are not expected to review or perform detailed tests of all financial or other systems and processes or of all accounting procedures and transactions;

(c) have regard to the fact that local government bodies operate and deliver their services in a range of partnerships and other forms of joint working or contracts with other public sector, voluntary or private sector bodies. Auditors should therefore consider whether they need to follow public money into and across such arrangements;

(d) discuss with the audited body the need for timely and effective production of working papers and other information required for audit so that the process can be carried out as efficiently and effectively as possible.

[…]

Confidentiality

12 Auditors should take all reasonable steps to ensure that they and their staff comply with relevant statutory and other requirements relating to the holding and disclosure of information received or obtained during the audit.

Auditing the financial statements

15 Auditors are required to audit the financial statements and to give their opinion, including:

(a) whether they present fairly, or, for local probation boards, give a true and fair view of, the financial position of the audited body and its expenditure and income for the year in question;

(b) whether they have been prepared properly in accordance with relevant legislation and applicable accounting standards; and

(c) for local probation boards, on the regularity of their expenditure and income.

16 In carrying out this responsibility, auditors should provide reasonable assurance that the financial statements:

(a) are free from material mis-statement, whether caused by fraud or other irregularity or error;

(b) comply with statutory and other applicable requirements; and

(c) comply with all relevant requirements for accounting presentation and disclosure.

17 Auditors should review whether the statement on internal control has been presented in accordance with relevant requirements and they should report if the statement:

- does not meet these requirements;
- is misleading; and/or
- is inconsistent with, or incomplete in the light of, other information of which the auditor is aware.

In doing so auditors should take into account the knowledge of the audited body that they gain through carrying out audit work in relation to the body's arrangements for securing economy, efficiency and effectiveness in its use of resources.

Risks identified by the Commission

29 The Commission may identify risks relating to the use of resources faced by all local government bodies of a particular type or within a locality. In the light of these risks the Commission may develop programmes of work or studies that require comprehensive coverage by auditors to enable comparisons to be made. The Commission may specify additional elements of work, to be carried out by auditors, which supplement the local risk-based approach to planning the audit.

Outputs from the audit

30 The results of audit work will be reported in a range of outputs that, unless specified otherwise, should be addressed to the audited body.

31 The following outputs should be issued at key points in the audit process:

(a) audit planning document;

(b) oral and/or written reports or memoranda to officers and, where appropriate, members on the results of, or matters arising from, specific aspects of auditors' work;

(c) a report to those charged with governance summarising the conclusions of the auditor;

(d) an audit report including the auditor's opinion on the financial statements and a conclusion on whether the audited body has put in place proper arrangements for securing economy, efficiency and effectiveness in its use of resources. For best value authorities this conclusion incorporates the auditor's report on the audit of the best value performance plan;

(e) a certificate that the audit of the accounts has been completed in accordance with statutory requirements; and

(f) an annual audit letter or, for those bodies where the Commission carries out inspections, information to be reported to the Commission in a specified format to enable it to prepare an annual audit and inspection letter to the audited body.

Principles of audit reporting

33 Auditors should maintain regular communications with audited bodies and ensure that emerging findings are discussed at the level within the audited body which auditors consider to be the most appropriate and on a timely basis.

35 Auditors should report to the audited body in such a way as to enable its members or officers to understand:

- the nature and scope of the audit work;
- any significant issues arising from auditors' work;
- the nature and grounds for any concerns they have; and
- where appropriate, any action that needs to be taken by the audited body to secure improvement.

Appendix 3

Audit Commission Act 1998

Section 6 Auditors' right to documents and information

(1) An auditor has a right of access at all reasonable times to every document relating to a body subject to audit which appears to him necessary for the purposes of his functions under this Act.

(2) An auditor may –

(a) require a person holding or accountable for any such document to give him such information and explanation as he thinks necessary for the purposes of his functions under this Act; and

(b) if he thinks it necessary, require the person to attend before him in person to give the information or explanation or to produce the document.

(4) Without prejudice to subsection (2), the auditor may –

(a) require any officer or member of a body subject to audit to give him such information or explanation as he thinks necessary for the purposes of his functions under this Act; and

(b) if he thinks it necessary, require the officer or member to attend before him in person to give the information or explanation.

(5) Without prejudice to subsections (1) to (4), every body subject to audit shall provide the auditor with every facility and all information which he may reasonably require for the purposes of his functions under this Act.

(6) A person who without reasonable excuse fails to comply with any requirement of an auditor under subsection (1), (2) or (4) is guilty of an offence and liable on summary conviction –

(a) to a fine not exceeding level 3 on the standard scale, and

(b) to an additional fine not exceeding £20 for each day on which the offence continues after conviction for that offence.

(7) Any expenses incurred by an auditor in connection with proceedings for an offence under subsection (6) alleged to have been committed in relation to the audit of the accounts of any body, so far as not recovered from any other source, are recoverable from that body.

Section 49 Restriction on disclosure of information

(1) No information relating to a particular body or other person and obtained by the Commission or an auditor, or by a person acting on behalf of the Commission or an auditor, pursuant to any provision of this Act or of Part I of the Local Government Act 1999 or in the course of any audit or study under any such provision shall be disclosed except –

(a) with the consent of the body or person to whom the information relates;

(b) for the purposes of any functions of the Commission or an auditor under this Act or under Part I of the 1999 Act;

(ba) to the Commission for Social Care Inspection for the purposes of its functions under Chapter 5 of Part 2 of the Health and Social Care (Community Health and Standards) Act 2003;

(bb) to the National Assembly for Wales for the purposes of its functions under Chapter 4 of that Part of that Act;

(c) in the case of a health service body, for those purposes or for the purposes of the functions of the Secretary of State and the Comptroller and Auditor General under the National Health Service Act 1977, or for the purposes of the functions the Commission for Healthcare Audit and Inspection under Chapter 3 of Part 2 of the Health and Social Care (Community Health and Standards) Act 2003;

(d) for the purposes of the functions of the Secretary of State relating to social security;

(da) for the purposes of any function of the Auditor General for Wales under the Public Audit (Wales) Act 2004 or (in relation to a health service body) under the Government of Wales Act 1998;

(dd) to the Mayor of London, where the information relates to the Greater London Authority or a functional body;

(dd)

(de) for the purposes of the functions of an ethical standards officer or the Public Services Ombudsman for Wales under Part 3 of the Local Government Act 2000;

(e) …

(f) for the purposes of any criminal proceedings.

(2) References in subsection (1) to studies and to functions of the Commission do not include studies or functions under section 36.

(3) A person who discloses information in contravention of subsection (1) is guilty of an offence and liable –

(a) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both; or

(b) on conviction on indictment, to imprisonment for a term not exceeding two years or to a fine or to both.

Section 49A Disclosure of information by or on behalf of public authorities

(1) This section applies if information relating to a particular body or other person is obtained by the Commission or an auditor, or a person acting on behalf of the Commission or an auditor –

(a) pursuant to a provision of this Act or of Part 1 of the Local Government Act 1999, or

(b) in the course of an audit of study under this Act or under Part 1 of the Local Government Act 1999.

(2) A person who is, or acts on behalf of a person who is, a public authority for the purposes of the Freedom of Information Act 2000, may disclose any such information –

(a) in the circumstances in which he would (but for section 49A(1)) be authorised to do so under section 49(1);

(b) in accordance with section 41(4); or

(c) in any other circumstances, except where such a disclosure would, or would be likely to, prejudice the effective performance by such a person of a function imposed or conferred on the person by or under an enactment.

(3) A person mentioned in subsection (2) who discloses any such information otherwise than as authorised by subsection (2) is guilty of an offence and liable on summary conviction to a fine not exceeding the statutory maximum.

Appendix 4

Relevant parts of sections 29, 35 and 55 of the Data Protection Act 1998

Section 29 Crime and taxation

(1) Personal data processed for any of the following purposes –

(a) the prevention or detection of crime,

(b) the apprehension or prosecution of offenders, or

(c) the assessment or collection of any tax or duty or of any imposition of a similar nature,

are exempt from the first data protection principle (except to the extent to which it requires compliance with the conditions in Schedules 2 and 3) and section 7 in any case to the extent to which the application of those provisions to the data would be likely to prejudice any of the matters mentioned in this subsection.

[…]

(3) Personal data are exempt from the non-disclosure provisions in any case in which –

(a) the disclosure is for any of the purposes mentioned in subsection (1), and

(b) the application of those provisions in relation to the disclosure would be likely to prejudice any of the matters mentioned in that subsection.

Section 35 Disclosures required by law or made in connection with legal proceedings etc

(1) Personal data are exempt from the non-disclosure provisions where the disclosure is required by or under any enactment, by any rule of law or by the order of a court.

Section 55 Unlawful obtaining etc of personal data

(1) A person must not knowingly or recklessly, without the consent of the data controller,

(a) obtain or disclose personal data or the information contained in personal data, or

(b) procure the disclosure to another person of the information contained in personal data.

(2) Subsection (1) does not apply to a person who shows –

(a) that the obtaining, disclosing or procuring –

(i) was necessary for the purpose of preventing or detecting crime, or

(ii) was required or authorised by or under any enactment, by any rule of law or by the order of a court,

(b) that he acted in the reasonable belief that he had in law the right to obtain or disclose the data or information or, as the case may be, to procure the disclosure of the information to the other person,

(c) that he acted in the reasonable belief that he would have had the consent of the data controller if the data controller had known of the obtaining, disclosing or procuring and the circumstances of it, or

(d) that in the particular circumstances the obtaining, disclosing or procuring was justified as being in the public interest.

(3) A person who contravenes subsection (1) is guilty of an offence.

(4) A person who sells personal data is guilty of an offence if he has obtained the data in contravention of subsection (1).

(5) A person who offers to sell personal data is guilty of an offence if –

(a) he has obtained the data in contravention of subsection (1), or

(b) he subsequently obtains the data in contravention of that subsection.

(6) For the purposes of subsection (5), an advertisement indicating that personal data are or may be for sale is an offer to sell the data.

(7) Section 1(2) does not apply for the purposes of this section; and for the purposes of subsections (4) to (6), "personal data" includes information extracted from personal data.

(8) References in this section to personal data do not include references to personal data which by virtue of section 28 (or 33A) are exempt from this section.

This report is available on our website at **www.audit-commission.gov.uk**. Our website contains a searchable version of this report, as well as a text-only version that can easily be copied into other software for wider accessibility.

If you require a copy of this report in large print, in braille, on tape, or in a language other than English, please call **0845 0522613**.

To order additional copies of this report or other Audit Commission publications please contact **Audit Commission Publications, PO Box 99, Wetherby, LS23 7SA Tel 0800 502030**.

Audit Commission
1st Floor, Millbank Tower,
Millbank, London SW1P 4HQ
Tel: 020 7828 1212 Fax: 020 7976 6187
Textphone (minicom): 020 7630 0421
www.audit-commission.gov.uk

Stock code: XXXXXX