

Code of data matching practice 2010

Issued under Section 26F of the Public Finance and
Accountability (Scotland) Act 2000 (as amended)



Prepared by Audit Scotland
November 2010

Audit Scotland is a statutory body set up in April 2000 under the Public Finance and Accountability (Scotland) Act 2000. It provides services to the Auditor General for Scotland and the Accounts Commission. Together they ensure that the Scottish Government and public sector bodies in Scotland are held to account for the proper, efficient and effective use of public funds.

Contents

**Foreword by the Accountable
Officer, Audit Scotland**
Page 2

**Foreword by the Information
Commissioner**
Page 3

Part 1. Introduction to the Code
Page 4

**Part 2. The Code of data matching
practice**
Page 7

**Part 3. Compliance with the Code
and the role of the Information
Commissioner**
Page 15

**Appendix 1. Definitions of terms
used in the Code**
Page 17

**Appendix 2. Examples of good
practice layered privacy notices for
public bodies**
Page 18

**Appendix 3. Extracts from
statutory provisions**
Page 24

Foreword by the Accountable Officer, Audit Scotland

Since it began in the 1990s, the National Fraud Initiative (NFI) has helped public bodies to identify fraud and error overpayments and other outcomes valued at more than £660 million across the UK. Scotland's share of this is around £58 million.

While the NFI exercise was originated by the Audit Commission, and it continues for now to play the major role in data processing and development, it now also involves the Wales Audit Office, the Northern Ireland Audit Office, as well as Audit Scotland. It remains a very successful example of efficient joined-up working among the UK audit agencies and the public bodies they audit.

Explicit powers to undertake data matching exercises were provided to the other UK audit agencies in the Serious Crime Act 2007. We are therefore pleased that the Scottish Government has now provided Audit Scotland with broadly equivalent provisions in Section 97 of the Criminal Justice and Licensing (Scotland) Act 2010, which commenced on 6 October 2010.

As well as providing Audit Scotland with explicit powers for data matching for the prevention and detection of fraud, and other specified purposes, the new legislation quite rightly includes safeguards for those individuals whose data is submitted for data matching. These include a

requirement for Audit Scotland to prepare and keep under review a Code of data matching practice, after consulting our audited bodies and the Information Commissioner.

Audit Scotland is grateful to the Information Commissioner's Office for its advice on the Code and to the Commissioner, personally, for agreeing to provide his own foreword to the Code.

The Code sets out the principles and practices that should be adopted by those taking part in NFI in Scotland. Key aspects of the Code include examples of how individuals should be informed that their personal information will be used for data matching, and how data will be submitted by bodies, and data matches provided to them, through an encrypted and password protected online system which meets UK government security standards for restricted data.

The Code comes into immediate effect and applies to Audit Scotland, the Audit Commission which processes data on our behalf, participating bodies in Scotland and the appointed external auditors who monitor their participation.



Robert W Black

Robert W Black
Accountable Officer, Audit Scotland

Foreword by the Information Commissioner

As UK Information Commissioner, I have responsibility for ensuring compliance with the Data Protection Act. In that capacity, I welcome the opportunity to contribute a foreword to Audit Scotland's Code of data matching practice.

All public bodies have a duty to ensure that they safeguard public money and minimise levels of fraud. This is particularly important when resources are tight. At the same time, public bodies must ensure that they deliver help to those entitled to receive it.

Data matching exercises help organisations meet both these objectives by identifying where inconsistencies in data may exist and highlighting any need for further investigation. But it is vital that the data matching tool is applied in the context of data protection law. Hence the need for this Code.

In most cases, the personal information checked in data matching will not reveal any inconsistencies. Sometimes, data matching will indicate an error that can quickly be put right, for example, where an individual may inadvertently have failed to inform the authorities of a change in circumstances.

But data matching may also point to a deliberate act by someone who intended to commit fraud.

By following the Code, public bodies will ensure that the innocent are properly protected while fraudulent claims are stopped.

I particularly welcome the statutory provision which requires Audit Scotland to consult with the ICO during the preparation of its Code of data matching practice. I am satisfied that it properly places the governance and application of data matching within the obligations put upon all organisations processing personal data by the Data Protection Act 1998. It also draws upon guidance issued by my office which helps to make such processing transparent and understandable to individuals who may be affected by it.



Christopher Graham
Information Commissioner

Part 1. Introduction to the Code



1.1 Audit Scotland

1.1.1 Audit Scotland is a statutory body set up under Section 10 of the Public Finance and Accountability (Scotland) Act 2000 to provide assistance and support to the Auditor General for Scotland (AGS) and the Accounts Commission. Audit Scotland employs the staff (including auditors) and incurs the expenditure (including the fees charged by firms appointed as auditors) required to support the functions of the AGS and the Accounts Commission.

1.1.2 Section 26A of the Public Finance and Accountability (Scotland) Act 2000 provides that Audit Scotland may carry out data matching exercises, or arrange for them to be carried out on its behalf. In practice, most of Audit Scotland's data matching will be done as part of joint exercises such as the National Fraud Initiative which is undertaken with the Audit Commission and the other UK public sector audit agencies. The key aspects of these exercises, such as the collection and processing of data, will usually be undertaken by the Audit Commission and any firm with which it is contracted, on behalf of Audit Scotland and the other audit agencies.

1.2 The Accounts Commission

1.2.1 The Accounts Commission is responsible, among other things, for appointing auditors to local government bodies in Scotland. The Local Government (Scotland) Act 1973 requires the Accounts Commission to appoint auditors to each audited body.

1.3 The Auditor General for Scotland

1.3.1 The Auditor General for Scotland (AGS) is responsible for deciding who should audit most of the other public bodies in Scotland, including NHS bodies, further education colleges, Scottish Water, the Scottish Government, government agencies

and non-departmental public bodies in Scotland. The Public Finance and Accountability (Scotland) Act 2000 requires the AGS to appoint auditors to each audited body outside the local government sector.

1.3.2 The AGS is also currently the Accountable Officer for Audit Scotland.

1.4 Background to the National Fraud Initiative

1.4.1 It is essential that public bodies have adequate controls in place to prevent and detect fraud and error. Fraud in local government, the health service and other public bodies is a major concern of those bodies as well as of Audit Scotland and those appointed by the AGS or the Accounts Commission to audit those bodies.

1.4.2 The National Fraud Initiative, known as NFI, is a data matching exercise that has been operated in England by the Audit Commission since 1996. The NFI assists audited bodies to prevent and detect fraud and error, and also helps auditors to assess the arrangements that audited bodies have put in place to deal with fraud. In conjunction with the Audit Commission, the NFI has been introduced in stages by Audit Scotland since 2000.

1.4.3 Data matching in the NFI involves comparing sets of data, such as the payroll or benefits records of a body, against other records held by the same or another body to see how far they match. The NFI will aim to avoid processing large amounts of personal data where there is not a significant risk of fraud being present. However, to allow potentially fraudulent claims and payments to be identified it is necessary for the personal data of honest individuals also to be processed.

1.4.4 Where no match is found, the data matching process has no material impact on those concerned. Where a match is found it indicates

that there may be an inconsistency that requires further investigation. In the NFI, participating bodies receive a report of matches that they should follow up, and investigate where appropriate, to detect instances of fraud, over or under-payments and other errors, to take remedial action and to update their records accordingly.

1.5 The statutory framework

1.5.1 Prior to 2010, data matching (NFI) operated in Scotland mainly under a combination of auditors' powers of access to information in Section 100 of the Local Government (Scotland) Act 1973 and Section 53 of the Local Government in Scotland Act 2003.

1.5.2 From 2010, Audit Scotland will conduct data matching exercises under statutory powers added to the Public Finance and Accountability (Scotland) Act 2000 by Section 97 of the Criminal Justice and Licensing (Scotland) Act 2010.

1.5.3 Under the new legislation:

(a) Audit Scotland may carry out data matching exercises for the purpose of assisting in the prevention and detection of fraud or other crime and in the apprehension and prosecution of offenders (referred to hereafter as the 'permitted purposes')

(b) Audit Scotland may require specified persons to provide data for data matching exercises. These include all the bodies to which the AGS or the Accounts Commission appoints auditors, licensing boards, and officers, office holders and members of these bodies or boards

(c) other persons or bodies may participate in Audit Scotland's data matching exercises on a voluntary basis. Where they do so, the statute states that there is no breach of confidentiality and generally removes other restrictions in providing the data to Audit Scotland

(d) the requirements of the Data Protection Act 1998 continue to apply

(e) Audit Scotland may disclose the results of data matching exercises where this assists the purpose of the matching (see (a) above), including disclosure to bodies that have provided the data and to the auditors appointed by the AGS and the Accounts Commission

(f) Audit Scotland may disclose both data provided for data matching and the results of data matching to the AGS, the Accounts Commission, the Audit Commission, or any of the other UK public sector audit agencies specified in Section 26D of the Public Finance and Accountability (Scotland) Act 2000, for the purposes described at (a) above

(g) wrongful disclosure of data obtained for the purposes of data matching by any person is a criminal offence

(h) Audit Scotland may impose reasonable charges on any body participating in a data matching exercise

(i) Audit Scotland must prepare and publish a Code of Practice with respect to data matching exercises. All bodies conducting or participating in its data matching exercises, including Audit Scotland itself, must have regard to this Code

(j) Audit Scotland may report publicly on its data matching activities.

1.6 Structure of the Code

1.6.1 The order in which the Code is set out reflects the chronological stages of a data matching exercise. This is designed to make it accessible to participating bodies.

1.6.2 Certain terms used in the Code are defined at [Appendix 1](#). These terms appear in bold text for ease of identification.

1.7 Review of the Code

1.7.1 Audit Scotland is required to keep the Code under review. It intends to update the Code in the light of changes in the law and to reflect comments and experience drawn from each data matching exercise.

1.8 Relationship of this Code to other information sharing codes

1.8.1 When participating in data matching exercises, bodies should have regard to any other relevant information sharing codes and guidance, including guidance from the Information Commissioner, as well as this Code.

1.9 Reproducing the Code

1.9.1 Bodies participating in data matching exercises may reproduce the text of this Code as necessary to ensure that all those involved are aware of their obligations in law and under this Code.

1.10 Queries on the Code

1.10.1 Any questions about this Code or a particular data matching exercise should be addressed to the Assistant Auditor General, Audit Scotland, 110 George Street, Edinburgh, EH2 4LH; tel 0845 146 1010. Email enquiries should be addressed to: info@audit-scotland.gov.uk and quote 'National Fraud Initiative' in the subject line.

1.11 Complaints

1.11.1 Complaints about bodies that are participating in Audit Scotland's data matching exercises should be addressed to the bodies themselves. Complaints about Audit Scotland's role in conducting data matching exercises will be dealt with under its complaints procedure.

1.11.2 The procedure asks that you first give Audit Scotland a chance to deal with a complaint informally. For NFI purposes please contact the officer mentioned at 1.10 above. If

you need any further help or advice, or are not satisfied with the way in which your informal enquiry was dealt with, please contact Audit Scotland on 0845 146 1010 or email us at: complaints@audit-scotland.gov.uk

1.11.3 If you wish to make a formal complaint, please refer to the complaints procedure which is on our website at: <http://www.audit-scotland.gov.uk/utilities/complaints.php> A formal complaint should be made on the complaints form, which may be downloaded from the same web page and posted or emailed back to Audit Scotland. If you would like assistance in completing the form, please let us know.

Part 2. The Code of data matching practice



2.1 Status, scope and purpose

2.1.1 This Code has been drawn up by Audit Scotland following a consultation process, as required by Section 26F of the Public Finance and Accountability (Scotland) Act 2000. It replaces the Code published in July 2006 and applies from the publication date until such time as a replacement Code is prepared.

2.1.2 This Code applies to all data matching exercises conducted by or on behalf of Audit Scotland under Part 2A of the Public Finance and Accountability (Scotland) Act 2000 for the purpose of assisting in the prevention and detection of fraud or other permitted purposes.

2.1.3 Any person or body conducting or participating in Audit Scotland's data matching exercises must, by law, have regard to the provisions of this Code.

2.1.4 The purpose of this Code is to help ensure that Audit Scotland and its staff, **auditors** and all persons and bodies involved in data matching exercises comply with the law, especially the provisions of the Data Protection Act 1998. The Code also aims to promote good practice in data matching. It includes guidance on the notification process for letting individuals know why their data is matched and by whom, the standards that apply and where to find further information.

2.1.5 This Code does not apply to the detailed steps taken by a **participant** to investigate matches from a data matching exercise. It is for **participants** to investigate matches in accordance with their usual practices for investigation of fraud and error etc.

2.1.6 The Information Commissioner regards the provisions of the Code as demonstrating a commitment to good practice standards that will help organisations to comply with data protection principles.

2.2 What is data matching?

2.2.1 The Public Finance and Accountability (Scotland) Act 2000 (the 2000 Act) and complementary legislation applying to other UK public sector audit agencies defines data matching as the comparison of sets of data to determine how far they match. In the 2000 Act, the purpose of data matching is to identify potential inconsistencies that may indicate fraud or assist with the other permitted purposes.

2.2.2 Where a match is found it indicates that there may be an inconsistency or circumstance that requires further investigation. No assumption can be made as to whether there is fraud, error or other explanation until an investigation is carried out by the **participant**.

2.2.3 The data compared are usually personal data. Personal data may only be obtained and processed in accordance with the Data Protection Act 1998.

2.3 Who will be participating?

2.3.1 Under the Public Finance and Accountability (Scotland) Act 2000, Audit Scotland may require all **audited bodies** in Scotland, and other specified persons, to provide data for data matching exercises. This includes all the bodies to which the AGS or the Accounts Commission appoints auditors. Bodies required to participate in this way are referred to in this Code as **mandatory participants**.

2.3.2 Where it considers it appropriate, Audit Scotland may also accept data from **voluntary participants**.

2.4 Governance arrangements

Nominated officers

2.4.1 The Director of Finance or equivalent senior named officer of each **participant** should act as **senior responsible officer** for the purposes of data matching exercises.

2.4.2 The **senior responsible officer** should nominate officers responsible for data handling, for follow-up investigations and to act as a **key contact** with Audit Scotland and **auditors**, and should ensure that they are suitably qualified and trained for their role.

2.4.3 **Participants'** data protection officers should be involved at an early stage in the arrangements for data handling, training and providing privacy notices.

2.4.4 The Assistant Auditor General has overall responsibility for data matching exercises at Audit Scotland. He can be contacted at Audit Scotland, 110 George Street, Edinburgh, EH2 4LH; tel 0845 146 1010 or by email at: info@audit-scotland.gov.uk quoting 'National Fraud Initiative' in the subject line. The day-to-day coordination of data matching exercises is led by a senior manager in the Audit Strategy Group who liaises with the Head of NFI and the NFI team at the Audit Commission, which matches the data on Audit Scotland's behalf.

Audit Scotland guidance

2.4.5 For each data matching exercise, Audit Scotland will issue instructions and guidance to all **participants**. This will set out the detailed responsibilities and requirements for participation. The most up-to-date instructions (formerly referred to as handbooks) can be found on Audit Scotland's website at: <http://www.audit-scotland.gov.uk/work/nfi.php>

2.4.6 Instructions and guidance for **participants** will include:

- (a) a list of the responsibilities of the nominated officers at the **participant**
- (b) specifications for each set of data to be included in the data matching exercise
- (c) any further requirements and returns concerning the data to be provided

(d) a timetable for processing

(e) information on how to confirm compliance with data protection requirements.

Secure NFI website

2.4.7 The Audit Commission has made available to Audit Scotland and **participants** a secure, password protected and encrypted website for data matching exercises, known as the secure NFI website. This site allows **participants** to transmit data securely to Audit Scotland (in practice to the Audit Commission which matches the data on behalf of Audit Scotland) and for the results of data matching to be made available in secure conditions. **Participants** also have access to further guidance material and training modules on this website, including reports on the quality of their data and information on how to interpret matches, and on co-operation between **participants**.

Notification by data controllers of processing purposes

2.4.8 The Information Commissioner maintains a public register of data controllers that process data covered by the Data Protection Act 1998. Data controllers determine the purpose and manner in which personal data will be processed. Each register entry includes the name and address of the data controller, the purposes for which data is processed, and specified information in relation to each purpose. Those data controllers that are required to notify, but fail to do so, are committing a criminal offence. It is the responsibility of all **participants**, both **mandatory** and **voluntary** (if any), to ensure that their notification to the Information Commissioner covers Audit Scotland and **auditors** as recipients against the appropriate purpose(s), ie for most audited bodies, the prevention and detection of fraud but also, when relevant, any other permitted purpose.

2.4.9 A notification handbook, which sets out how to complete the required notification form, is available from the Information Commissioner's

Office. Notification templates are available from the Information Commissioner for local authorities, NHS and other public bodies.

2.5 How Audit Scotland chooses data to be matched

2.5.1 Audit Scotland will only choose data sets to be matched where it has reasonable evidence that one of the data matching purposes permitted by the Public Finance and Accountability (Scotland) Act 2000 will be met as a result of matching those data sets. This will be a key consideration when Audit Scotland decides whether it is appropriate to accept data from a **voluntary participant**, or to require data from a **mandatory participant**. Evidence may come from previous data matching exercises, pilot exercises, from **participants** themselves or from other reliable sources of information such as **auditors** and the police.

2.5.2 Audit Scotland will undertake new areas of data matching on a pilot basis to test their effectiveness in serving the permitted purposes. Such pilots will be subject to a privacy impact assessment and only where pilots achieve matches that demonstrate a significant level of success (eg, potential fraud) should they be extended nationally. A small number of serious incidents of fraud or a larger number of less serious ones may both be treated as significant. The terms of this Code apply in full to pilot exercises. Pilot data must be provided in accordance with the provisions of the Data Protection Act 1998.

2.5.3 Audit Scotland may also undertake data matching based on the results of previous data matching exercises or pilot exercises that have been undertaken by the Audit Commission or one of the other UK public sector audit agencies.

2.5.4 Audit Scotland (or the Audit Commission) will review the results of each exercise in order to refine how it chooses the data for future exercises.

2.6 The data to be provided

2.6.1 The data required from **participants** will be the minimum needed to undertake the matching exercise, to enable individuals to be identified accurately and to report results of sufficient quality. This will be set out in the form of a data specification for each data set in the instructions for each exercise.

2.6.2 The **senior responsible officer** at each **participant** will normally be notified about any revisions to the data specifications at least six months before the data is to be provided. This is to ensure that **participants** have early notification of any changes so they can prepare adequately.

2.7 Powers to obtain and provide the data

2.7.1 All **mandatory participants** must provide data for data matching exercises as required by Audit Scotland. Failure to provide data without reasonable excuse is a criminal offence under Section 26C (5) of the Public Finance and Accountability (Scotland) Act 2000.

2.7.2 The provision of data to Audit Scotland by a **voluntary participant** does not amount to a breach of confidentiality, and generally does not breach other legal restrictions. This is provided for in Section 26B of the Public Finance and Accountability (Scotland) Act 2000. Section 26B provides the legal basis for a **voluntary participant** to comply with the 'fair and lawful' processing requirement of the first principle of the Data Protection Act.

2.7.3 Patient data may not be shared voluntarily, and so may only be used in data matching if Audit Scotland requires it from a **mandatory participant**.

2.7.4 Whether **participants** provide data on a mandatory or voluntary basis, they are still required to provide the data in accordance with the provisions of the Data Protection Act

1998. This means that the disclosure of data must be in accordance with the data protection principles unless a relevant exemption in the Data Protection Act 1998 has been applied.

2.7.5 In most cases, data matching will take place in accordance with the data protection principles with no need to rely on exemptions. The main exemptions in relation to obtaining and providing data are Sections 34 and 35 of the Data Protection Act 1998, which would need to be considered in the circumstances of each data matching exercise. Relevant extracts from the Data Protection Act 1998, including the data protection principles, are set out in [Appendix 3](#).

2.8 Fairness, privacy and transparency

2.8.1 The processing of data by Audit Scotland in a data matching exercise is carried out with statutory authority. It does not require the consent of the individuals concerned under the Data Protection Act 1998. The relevant provisions of the Data Protection Act 1998 are included in [Appendix 3](#).

Privacy notices

2.8.2 The Data Protection Act 1998 normally requires **participants** to inform individuals that their data will be processed. Unless an exemption applies, for data processing to be fair, the first data protection principle requires data controllers to inform individuals whose data is to be processed of:

- (a) the identity of the data controller
- (b) the purpose or purposes for which the data may be processed
- (c) any further information which is necessary to enable the processing to be fair.

2.8.3 The Information Commissioner's Office now promotes the use of the term 'privacy notice' to describe the provision of this information and that is the term used in this Code.

Previous documents have referred to 'fair processing notices' but the purpose and substance of the notice is the same. A privacy notice enables people to know that their data is being used for one of the permitted purposes (eg, the prevention and detection of fraud) and to take appropriate steps if they consider the use is unjustified, or unlawful in their particular case.

2.8.4 Participants should, so far as practicable, ensure that privacy notices are actively provided, or at least made readily available to the individuals about whom they are sharing information. The notice should clearly set out an explanation that their data may be disclosed for the purpose of preventing and detecting fraud (or other permitted purpose, as appropriate). The notice should state that the data will be provided to Audit Scotland for this purpose. The notice should also contain details of how individuals can find out more information about the processing in question.

2.8.5 Communication with individuals whose data is to be matched should be clear, prominent and timely. It is good practice for reminder notices to be issued before each round of data matching exercises.

2.8.6 When providing data to Audit Scotland, **participants** should submit a declaration, using the facility available on the NFI secure website, confirming compliance with the privacy notification requirements. However, if Audit Scotland or an **auditor** becomes aware that privacy requirements have not been adhered to, they should agree the steps necessary for the **participant** to achieve compliance.

Layered notices

2.8.7 The Information Commissioner recommends a layered approach to privacy notices. Usually there are three layers: *summary notice*, *condensed text* and *full text*. Taken together, the three layers comprise the privacy notice.

2.8.8 The *summary notice* should provide the minimum necessary content and should be provided to the individuals whose data is to be matched. Where practicable, it should point to where more detailed information can be found, for example, by providing web links to the second and third layers, or contact details for a named person such as the **key contact** or data protection officer. **Participants** should make clear where individuals can obtain further information about how, why and by whom their data is being processed.

2.8.9 In the case of benefits, licences and applications for services, for example, the summary notice should usually be included on the application form used to collect the data in the first place.

2.8.10 In other cases, such as occupational pensioners and tenants, **participants** usually communicate formally at least once a year, for example by newsletter. Summary notices should be included in these communications, which should be sent to named individuals in advance of each data matching exercise where practicable. This will avoid the cost of a separate mailing.

2.8.11 Participants should notify their employees both at the time of the original application for their post and before each exercise, for example, by including a summary notice in their payslip.

2.8.12 The *condensed text* should give a summary of Audit Scotland's data matching exercises, and should be available on the **participant's** website as well as in hard copy on request. This layer should provide a link to the more detailed full text.

2.8.13 The *full text* should be available on Audit Scotland's website and should include an explanation of the legal basis for its data matching exercises and a more detailed description of how the NFI works. The full text should also explain that

being included in a data matching exercise does not mean that individuals are under suspicion and that NFI also helps **participants** to meet their obligations under data protection legislation to ensure that their records are up to date.

2.8.14 While **participants** should decide the content and means of issue of privacy notices for themselves, good practice examples of a three-layered approach for **mandatory participants** are included at [Appendix 2](#). **Voluntary participants** should prepare and issue similar notices reflecting the nature of their participation, the relevant statutory provisions for voluntary bodies and removing the references that apply only to bodies within the public audit regime in Scotland. Such notices may have the effect of deterring fraud as well as informing applicants about the use of data in data matching.

2.8.15 The benefit of using a layered approach is to give appropriate levels of privacy information to different audiences, depending on their information needs. Individuals who wish to have a relatively short explanation can access this in a summary notice, while more comprehensive information can be made available for others.

Collection of new data

2.8.16 **Participants** should provide summary privacy notices at the point of collecting personal data where practicable. **Participants** should in any event provide such notices before disclosure of the data to Audit Scotland, unless it is impracticable to do so.

Retrospective privacy notices

2.8.17 It is sometimes not practicable to provide a summary privacy notice at the time of the original collection of the data. In such cases, **participants** should provide retrospective summary privacy notices at the earliest reasonable opportunity, and before disclosure to Audit Scotland. Where this is impracticable **participants** should maintain a record of the reasons.

Deceased persons

2.8.18 Some of the data used for data matching exercises relates to deceased persons. Although information relating to a deceased individual cannot be regarded as personal data of the deceased person under the Data Protection Act 1998, common law rules of confidentiality may restrict disclosure in certain circumstances. In order not to cause unnecessary distress or harm, particular care and sensitivity should be taken in dealing with data concerning deceased persons throughout the exercise, but particularly when investigating matches.

2.9 Quality of the data

2.9.1 **Participants** should ensure that the data they provide for data matching are of good quality (ie, accurate and complete). Processing of inaccurate data could mean that the **participant** is in breach of data protection law.

2.9.2 Before providing data for matching, **participants** should ensure that the data is as accurate and up to date as possible. Errors identified from previous data matching exercises should be rectified, and action taken to address any issues identified in data quality reports supplied to the **participant** on the secure NFI website.

2.10 Security

2.10.1 Audit Scotland, the Audit Commission (including any successor body) and any firm undertaking matching as its agent, and all **participants** must put in place security arrangements for handling and storing data in data matching exercises.

2.10.2 These arrangements should ensure that:

(a) specific responsibilities for security of data have been allocated to one or more managers

(b) security measures take appropriate account of the physical environment in which data is held, including the security of premises and storage facilities

(c) there are physical and logical controls to restrict access to data held electronically, so that only those named individuals who need to access the data for the purpose of data matching exercises can do so

(d) all staff with access to data are given training that is sufficient to enable them to appreciate why and how they need to protect the data. **Participants** should refer to the training modules on the secure NFI website

(e) if a breach of security occurs, or is suspected, authorised users are given new passwords or are required to change their passwords as soon as possible. The body responsible should consider what further steps it should take in the light of the Information Commissioner's guidance on management of security breaches.

Appropriate audit trails should be maintained, where practicable, to evidence that such arrangements are being complied with.

2.10.3 All persons handling data as part of the data matching exercise should be made aware of their data protection, confidentiality and security obligations. Such staff should be subject to strict access authorisation procedures. Breach of authorisation procedures should attract appropriate disciplinary sanctions.

2.10.4 The Audit Commission's secure NFI website is password protected and encrypted to 128 bit SSL standards both for the transmission of data to the Commission and the disclosure of the results of data matching to **participants**. The website also complies with UK government information standards and is formally accredited to handle, store and process information up to the required

'restricted' classification levels. Similar standards should apply to any other website or arrangement that may be made for these purposes.

2.10.5 Any firm processing data for the Audit Commission will do so under a contract in writing that imposes requirements as to technical and organisational security standards so as to meet ISO 27001/02, and under which the firm may only act on instructions from the Audit Commission. The Audit Commission, assisted by Audit Scotland and the other UK public sector audit agencies, will monitor the firm's compliance with these standards from time to time.

2.10.6 Where the Audit Commission undertakes data matching exercises on behalf of Audit Scotland or any other UK public sector audit agency there should be a similar written contract in place.

2.11 Supply of data to Audit Scotland

2.11.1 Participants should normally only submit data to Audit Scotland via the Audit Commission's secure NFI website or, in future, an approved alternative that has also been accredited against HM government security standards.

2.11.2 In exceptional cases, data may be submitted by an alternative method provided this satisfies the security requirements of the Code and is approved by the Audit Commission.

2.12 The matching of data by Audit Scotland

2.12.1 Audit Scotland will ensure that it matches data fairly and for a purpose permitted by the Public Finance and Accountability (Scotland) Act 2000, eg assisting in the prevention and detection of fraud or other permitted purpose.

2.12.2 The techniques used by Audit Scotland in data matching exercises should be those that are likely to assist with achieving a permitted purpose. They should be refined in the light of practical experience, having identified any lessons from reviewing the results of previous exercises.

2.12.3 All data stored electronically by Audit Scotland, or the Audit Commission or any firm contracted to process the data, will be held on a secure, password-protected computer system maintained in a secure environment.

2.12.4 The Audit Commission will undertake the processing of data on behalf of Audit Scotland. Any staff at the Audit Commission, or any firm undertaking data matching as its agent, who have access to source data that has been provided for the NFI exercise in Scotland, will be subject to security clearance to at least Baseline Personnel Security Standard (BPSS) level.

2.12.5 All data provided for the purpose of data matching exercises will be backed up by Audit Scotland, or the Audit Commission or any firm undertaking data matching as its agent, at appropriate intervals, as reasonably necessary. Back-ups will be subject to the same security, destruction and access controls as the original data.

2.13 Access to the results by the bodies concerned

2.13.1 All results from data matching exercises will normally be made available to **participants** via the Audit Commission's secure NFI website. The results comprise the computer data file of reported matches and other relevant information arising from processing the data. In exceptional cases, matches may be made available by an alternative method provided this satisfies the security requirements of the Code and is approved by the Audit Commission.

2.13.2 The **senior responsible officer** should ensure that the results of a data matching exercise are disclosed only to named officers for each type of result. The secure NFI website is designed for that purpose.

2.13.3 All results from data matching exercises held by a **participant** other than on the secure NFI website should be held on an equally secure, password protected and encrypted computer system. Any printed results should be kept in locked storage in a secure environment and should only be accessible to named individuals as referred to in 2.10.2 (c).

2.14 Following up the results

2.14.1 The detailed steps taken by a **participant** to investigate the results of data matching are beyond the scope of this Code. However, it is important to recognise that matches are not necessarily evidence of fraud or any other outcome related to the purpose for which the matching was undertaken. **Participants** should review the results to eliminate coincidental matches, and will want to concentrate on cases that are potentially fraudulent or otherwise indicative of the outcome for which the matching was undertaken. In the process, they will need to identify and correct those cases where errors have occurred.

2.14.2 No decision should be made as a result of a data match until the circumstances have been considered by an investigator at the **participant**. Investigating officers will find it helpful to refer to the guidelines on how to interpret matches and cooperation between bodies prepared by the Audit Commission, which are available to participants on its secure NFI website.

2.14.3 A data match between two (or more) **participants** may require the **participants** to share other information about the individual who is the subject of the match, before it would be possible to determine

whether or not a crime (including fraud) has occurred. Section 29(1) of the Data Protection Act 1998 permits such disclosure, for example, where the prevention or detection of crime would otherwise be likely to be prejudiced. [Appendix 3](#) includes extracts from Section 29. **Participants** may find it helpful to enter into data sharing arrangements before matches become available so that matches can be investigated without undue delay.

2.14.4 Participants should consider whether any corrections to personal data found to contain errors as a result of data matching are substantial enough to warrant notification to the persons concerned.

2.15 Disclosure of data used in data matching

2.15.1 Data obtained for the purpose of a data matching exercise may not be disclosed unless there is legal authority for so doing. This applies to both data obtained by Audit Scotland for the purposes of data matching exercises and the results of the data matching.

2.15.2 There is legal authority for Audit Scotland to disclose the data or results when this will assist in the prevention and detection of fraud or another permitted purpose. This includes, for example, disclosure of the results to the **participant** to investigate any matches, and disclosure to the **auditor**, for example, to assess the **participant's** arrangements for the prevention and detection of fraud.

2.15.3 Audit Scotland may also provide data matching results, for example, to the NHS Counter Fraud Service in Scotland which has the connected purpose, among other things, of assisting health bodies to interpret and follow up the results of Audit Scotland's data matching exercises.

2.15.4 Audit Scotland may also disclose data to the other public

sector audit agencies in England, Wales and Northern Ireland, to the bodies whose accounts they arrange to be audited, and to the **auditors** they appoint.

2.15.5 A body in receipt of data matching results from Audit Scotland may only disclose them further if it is to assist in the prevention and detection of fraud or another permitted purpose, to investigate and prosecute an offence, for the purpose of disclosure to an **auditor** or otherwise as required by statute.

2.15.6 The legal basis of these rules is Section 26D of the Public Finance and Accountability (Scotland) Act 2000 (see [Appendix 3](#)). Any disclosure by Audit Scotland, a **participant** or any person in breach of Section 26D is a criminal offence.

2.16 Access by individuals to data included in data matching

2.16.1 Individuals whose data is included in a data matching exercise may have rights of access to information under the Data Protection Act 1998 or Freedom of Information legislation. These should be dealt with in accordance with the organisation's general arrangements for responding to requests for information.

2.16.2 Individuals' usual rights of access to data held about them may be limited as a consequence of Section 29 of the Data Protection Act 1998, where disclosure would be likely to prejudice the prevention or detection of a crime or the apprehension or prosecution of an offender. This determination should be made on a case-by-case basis by the organisation in receipt of the request for information. This means that individuals may be refused full access to information about them that has been processed in data matching exercises.

2.16.3 Individuals have rights under the Data Protection Act 1998 if data held about them is inaccurate. They

should be able to check the accuracy of their data by contacting the **participant** holding the data.

2.16.4 Individuals should not expect to be told about data or data matches concerning any other person unless that person has given consent, as this is likely to amount to a breach of data protection principles.

2.16.5 Information requests under the Freedom of Information (Scotland) Act 2002 may be subject to the law enforcement exemption in Section 35, for example where its disclosure would be likely to prejudice substantially the prevention and detection of a crime or the apprehension or prosecution of an offender, or the personal information exemption under Section 38. These determinations should be made on a case by case basis by the organisation in receipt of the request for information.

2.16.6 Individuals who want to know whether their data is to be included in a data matching exercise can check the data specifications for each exercise in Audit Scotland's instructions. The most up to date instructions can be found on Audit Scotland's website at: <http://www.audit-scotland.gov.uk/work/nfi.php> or by contacting Audit Scotland (see 1.10 for contact details).

2.16.7 Participants should have arrangements in place for dealing with complaints from individuals about their role in a data matching exercise. If a **participant** receives a complaint and Audit Scotland is best placed to deal with it, the complaint should be passed on promptly to Audit Scotland.

2.16.8 Complaints about Audit Scotland's role in conducting data matching exercises will be dealt with under Audit Scotland's complaints procedure (see 1.11 for details).

2.17 Role of auditors

2.17.1 Where a **participant** is an **audited body** to which the Auditor General for Scotland (AGS) or the Accounts Commission appoints an **auditor**, the auditor will be concerned, among other things, to assess the arrangements that the body has in place to:

- (a) prevent and detect fraud generally
- (b) follow up and investigate NFI matches and act upon instances of fraud and error.

2.17.2 Where a **participant** does not have an **auditor** appointed by the AGS or the Accounts Commission, it is matter for the **participant** and its auditor to determine the role of the auditor in data matching and what disclosure to the auditor is appropriate.

2.18 Retention of data

2.18.1 Personal data should not be kept for longer than is necessary.

2.18.2 Access to the results of a data matching exercise on the secure NFI website will not be possible after a minimum reasonable period necessary for **participants** to follow up matches. Audit Scotland (or the Audit Commission on its behalf) will notify the end date of this period to **participants**.

2.18.3 **Participants** and their **auditors** may decide to retain some data after this period. Data may, for example, be needed as working papers for the purposes of audit, or for the purpose of continuing investigation or prosecution. **Participants** should consider what to retain in their individual circumstances in the light of any particular obligations imposed on them. **Mandatory participants**, to which the AGS or Accounts Commission appoints an **auditor**, should discuss with their **auditor** what should be retained for the purposes of audit. All **participants** should ensure that data no longer

required, including any data taken from the secure NFI website, are destroyed promptly and rendered irrecoverable. Data retained will be subject to the requirements of the Data Protection Act 1998.

2.18.4 All original data submitted to Audit Scotland (or the Audit Commission on its behalf) will be destroyed and rendered irrecoverable by the Audit Commission within six months of submission by the **participant**. Subject to paragraph 2.18.5 below, all data that are derived or produced from that original data, including data held by any firm undertaking data matching as the agent of Audit Scotland or the Audit Commission, will be destroyed and rendered irrecoverable within three months of the conclusion of the exercise.

2.18.5 A single set of reference codes for previous matches, together with any comments made by **participants'** investigators, will be retained securely offline by the Audit Commission for as long as they are relevant. This is solely for the purpose of preventing unnecessary re-investigation of previous matches in any subsequent data matching exercise.

2.19 Reporting of data matching exercises

2.19.1 Audit Scotland will prepare and publish a report on its data matching exercises from time to time. This will bring its data matching activities and a summary of the results achieved to the attention of the public.

2.19.2 Audit Scotland's report will not include any information obtained for the purposes of data matching from which a person or body may be identified, unless the information is already in the public domain. Audit Scotland may report on the progress of prosecutions resulting from data matching as these will be in the public domain.

2.20 Review of data matching exercises

2.20.1 Audit Scotland, in conjunction with the Audit Commission, will review the results of each exercise in order to refine how it chooses the data for future exercises and the techniques it uses.

2.20.2 As part of its review of each exercise, Audit Scotland should consider any complaints or representations made by **participants** or by people whose data has been processed during the exercise.

Part 3. Compliance with the Code and the role of the Information Commissioner



3.1 Compliance with the Code

3.1.1 Questions and concerns about non-compliance with the Code should be addressed to the organisation responsible in the first instance (that is to the **participant** or, if it concerns Audit Scotland's compliance, to Audit Scotland), before contacting the Information Commissioner.

3.1.2 Where Audit Scotland or an **auditor** becomes aware that a **participant** has not complied with the requirements of the Code, they should notify the body concerned and seek to ensure that it puts in place adequate measures to meet the Code's requirements. For example, this might include where a **participant** has not issued adequate privacy notices or submits data other than via the secure NFI website (and that exception has not been approved by the Audit Commission).

3.2 Role of the Information Commissioner

3.2.1 The Information Commissioner regulates compliance with the Data Protection Act 1998. If a matter is referred to the Information Commissioner, he or she would consider compliance with this Code by **participants** or Audit Scotland in determining the nature of any enforcement action. Guidance on the Information Commissioner's approach to enforcement and Data Protection Strategy is available on the Information Commissioner's Office's (ICO) website. Questions about the law and information sharing generally may be addressed to the Information Commissioner. In the first instance, public bodies in Scotland are advised to contact the ICO's regional office at:

The Information Commissioner's Office,
93-95 Hanover Street,
Edinburgh, EH2 1DJ
Tel: 0131 301 5071

The ICO's headquarters are at:

The Information Commissioner's Office,
Wycliffe House, Water Lane
Wilmslow, Cheshire, SK9 5AF
ICO helpline: 08456 30 60 60
01625 54 57 45

Email: mail@ico.gsi.gov.uk

Website: www.ico.gov.uk (use online enquiries form for questions regarding the legislation for which the Information Commissioner is responsible).

3.2.2 The Information Commissioner has been invited (under Section 51(7) of the Data Protection Act 1998) to review the Audit Commission's data matching exercises (and, in effect, the NFI exercises undertaken by Audit Scotland and the other UK public sector audit agencies) to assess compliance with the Data Protection Act 1998.

3.2.3 **Participants** are encouraged to invite the ICO to review their procedures. The purpose of this review would be to assess **participants'** compliance with data protection principles when processing personal data for the purposes of data matching exercises.

Appendix 1.

Definitions of terms used in the Code

For the purposes of this Code the following definitions apply:

Term	Definition
Auditor	A person in Audit Scotland or a private accountancy firm appointed under statute by the Accounts Commission or the Auditor General for Scotland (AGS) to act as an auditor in relation to an audited body.
Audited body	A local government or other body in Scotland to which the Accounts Commission or AGS appoints the auditor. This includes councils, police authorities, fire and rescue authorities, health bodies, Scottish Government and other bodies in the central government sector. Lists of audited bodies and auditors are available on Audit Scotland's website at: http://www.audit-scotland.gov.uk/about/as/audits.php
Key contact	The officer nominated by a participant's senior responsible officer to act as point of contact with Audit Scotland and auditors for the purposes of data matching exercises.
Mandatory participant	An audited body and other person specified in Section 26C of the Public Finance and Accountability (Scotland) Act 2000 that is required by Audit Scotland to provide data for a data matching exercise.
Voluntary participant	An organisation from which Audit Scotland considers it appropriate to accept data on a voluntary basis for the purposes of data matching.
Participant	An organisation that provides data to Audit Scotland for the purposes of a data matching exercise, which may be on either a mandatory or voluntary basis.
Patient data	Data relating to an individual that are held for medical purposes and from which the individual can be identified. This includes both clinical data (for example, the medical records) and demographic data (for example, the name and address) of patients.
Senior responsible officer	The Director of Finance or other senior named officer of the participant responsible for ensuring compliance with this Code.

Appendix 2.

Examples of good practice layered privacy notices for public bodies

The Information Commissioner recommends that a layered approach is adopted when issuing privacy notices. The purpose of each layer and the benefits of the approach are described in Section 2.8.

Participants in Audit Scotland's data matching exercises must decide for themselves the content and means of issue of privacy notices, but good practice examples for public bodies, where the purpose of the data matching is to assist in the prevention and detection of fraud, are set out below. Participants should seek to incorporate notices into existing forms of communication wherever possible.

Level 1 – Summary text

Example for application forms (for example, for benefits, housing tenancies, employment, market traders and taxi drivers)

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.

For further information, see {web link to Level 2 notice on participant's website} or contact {name and contact details in participant}.

Level 1 – Summary text

Example for payslips (for employees)

Please note that key payroll data may* be provided to bodies responsible for auditing and administering public funds for the purposes of preventing and detecting fraud. For more details, see {web link to Level 2 notice on participant's website} or contact {name and contact details in participant}.

* 'May' in this context means 'permitted' but if participants consider that it would avoid ambiguity they may prefer to use 'will' instead. However, 'may' is more appropriate, for example, when revising the wording on applications, especially if the data is not yet required by Audit Scotland for data matching purposes.

Level 1 – Summary text

Example for letters (for example, to pensioners, employees and tenants, where communication by newsletter, payslip and so on is not practicable)

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

Dear {name [of pensioner]}

THIS LETTER IS FOR INFORMATION ONLY – YOU ARE NOT REQUIRED TO TAKE ANY ACTION

{Name of Participant} is participating in an exercise to promote the proper spending of public money.

We are required by law to protect the public funds we administer. We may share information provided to us with other bodies responsible for auditing or administering public funds in order to prevent and detect fraud.

Audit Scotland currently requires us to participate in its anti-fraud initiative. For this initiative, we are providing details of [pensioners] so that they can be compared with information provided by other public bodies. This will ensure, for example, that [no pensions are being paid to persons who are deceased or no longer entitled, and that occupational pension income is being declared when housing benefit is applied for].

Sometimes wrong payments are made because of a genuine error. Previous exercises have uncovered instances of [pensioners] receiving too little [pension], resulting in the payments to [pensioners] being increased. These exercises, therefore, help promote the best use of public funds.

You do not need to respond to this letter. You may be contacted again in the future if the exercise suggests you are not receiving the correct amount of [pension]. Further information is available on our website at {participant's web link}. However, if you have any questions you should contact {name and contact details in participant}, who can also provide hard copies of information available on our website.

Level 2 – Condensed text**To be published on participant's website**

This authority is required by law to protect the public funds it administers. It may share information provided to it with other bodies responsible for auditing or administering public funds, in order to prevent and detect fraud.

On behalf of {the Accounts Commission/the Auditor General for Scotland – delete as appropriate}, Audit Scotland appoints the auditor to audit the accounts of this authority. It is also responsible for carrying out data matching exercises.

Data matching involves comparing computer records held by one body against other computer records held by the same or another body to see how far they match. This is usually personal information. Computerised data matching allows potentially fraudulent claims and payments to be identified but the inclusion of personal data within a data matching exercise does not mean that any specific individual is under suspicion. Where a match is found it indicates that there may be an inconsistency that requires further investigation. No assumption can be made as to whether there is fraud, error or other explanation until an investigation is carried out. The exercise can also help bodies to ensure that their records are up to date.

Audit Scotland currently requires us to participate in a data matching exercise to assist in the prevention and detection of fraud. We are required to provide particular sets of data to Audit Scotland for matching for each exercise, and these are set out in Audit Scotland's instructions, which can be found at: <http://www.audit-scotland.gov.uk/work/nfi.php>

The use of data by Audit Scotland in a data matching exercise is carried out with statutory authority, normally under its powers in Part 2A of the Public Finance and Accountability (Scotland) Act 2000. It does not require the consent of the individuals concerned under the Data Protection Act 1998.

Data matching by Audit Scotland is subject to a Code of Practice. This may also be found at: <http://www.audit-scotland.gov.uk/work/nfi.php>

For further information on Audit Scotland's legal powers and the reasons why it matches particular information, see the full text privacy notice at: <http://www.audit-scotland.gov.uk/work/nfi.php> or contact {name and contact details in participant}.

Level 3 – Full text

To be published on Audit Scotland's website

Audit Scotland data matching exercises**Introduction**

Audit Scotland conducts data matching exercises to assist in the prevention and detection of fraud. This is one of the ways in which Audit Scotland meets its responsibility of promoting economy, efficiency and effectiveness in the use of public money.

Data matching involves comparing sets of data, such as the payroll or benefits records of a body, against other records held by the same or another body. The data is usually personal information. The data matching allows potentially fraudulent claims and payments to be identified but the inclusion of personal data within a data matching exercise does not mean that any specific individual is under suspicion. Where a match is found it indicates that there may be an inconsistency which requires further investigation. No assumption can be made as to whether there is fraud, error or other explanation until an investigation is carried out. The exercise can also help bodies to ensure that their records are up to date.

The processing of data by Audit Scotland (in practice the processing is undertaken by the Audit Commission on Audit Scotland's behalf) in a data matching exercise is normally carried out under the powers in Part 2A of the Public Finance and Accountability (Scotland) Act 2000. It does not require the consent of the individuals concerned under the Data Protection Act 1998.

All bodies participating in Audit Scotland's data matching exercises receive a report of matches that they should investigate, so as to detect instances of fraud, over or under-payments and other errors, to take remedial action and update their records accordingly.

Since 2000, Audit Scotland's National Fraud Initiative (NFI) has led to the detection of fraud and overpayments totalling around £58 million. Across the UK, since 1996, all such exercises undertaken by the Audit Commission have led to the detection of fraud and overpayments totalling in excess of £660 million.

Legal basis

From 2010 Audit Scotland will normally conduct data matching exercises under its new statutory powers in Part 2A of the Public Finance and Accountability (Scotland) Act 2000. Previous exercises were conducted as part of the statutory audits and in accordance with duties placed on auditors by the Code of audit practice approved by the Accounts Commission and the Auditor General for Scotland (AGS).

Under the new powers:

(a) Audit Scotland may carry out data matching exercises for the purpose of assisting in the prevention and detection of fraud or other crime and in the apprehension and prosecution of offenders (the 'permitted purposes')

(b) Audit Scotland may require certain persons to provide data for data matching exercises. These persons include all the bodies to which the AGS or the Accounts Commission appoints auditors, licensing boards, and officers, office holders and members of these bodies or boards

(c) other persons or bodies may participate in Audit Scotland's data matching exercises on a voluntary basis. Where they do so, the statute states that there is no breach of confidentiality and generally removes other restrictions in providing the data to Audit Scotland

(d) the requirements of the Data Protection Act 1998 continue to apply

(e) Audit Scotland may disclose the results of data matching exercises where this assists the purpose of the matching (see (a) above), including disclosure to bodies that have provided the data and to the auditors appointed by the AGS and the Accounts Commission

(f) Audit Scotland may disclose both data provided for data matching and the results of data matching to the AGS, the Accounts Commission, the Audit Commission, or any of the other UK audit agencies specified in Section 26D of the Public Finance and Accountability (Scotland) Act 2000, for the purposes described at (a) above

(g) wrongful disclosure of data obtained for the purposes of data matching by any person is a criminal offence

(h) Audit Scotland may impose reasonable charges on any body participating in a data matching exercise

(i) Audit Scotland must prepare and publish a Code of Practice with respect to data matching exercises. All bodies conducting or participating in its data matching exercises, including Audit Scotland itself, must have regard to the Code

(j) Audit Scotland may report publicly on its data matching activities.

Bodies required to provide data for matching

Currently, Audit Scotland requires the following bodies to provide data for NFI in Scotland:

[List of audited bodies, to be updated by Audit Scotland from time to time]

In addition, the following bodies provide data to Audit Scotland for matching on a voluntary basis:

[List of voluntary bodies, if any, to be updated by Audit Scotland from time to time]

The data that are matched and the reasons for matching

For information describing which data sets are matched by Audit Scotland and the purpose of each match please refer to Audit Scotland's instructions available on the same web page as this notice and the table below which summarises the various match types for each participating organisation.

[Table to be included and updated from time to time to reflect the scope of each exercise]

Code of data matching practice

Data matching by Audit Scotland is subject to a Code of data matching practice. This may also be found on the same web page as this notice.

Further information

More details on Audit Scotland's data matching exercises, including national reports, other publications and guidance, may be found on the same web page as this notice.

Alternatively, please contact the senior manager (Audit Strategy and NFI), Audit Scotland, 110 George Street, Edinburgh, EH2 4LH; tel 0845 146 1010. Email enquiries should be addressed to: info@audit-scotland.gov.uk quoting 'National Fraud Initiative' in the subject line.

More information about the UK National Fraud Initiative is available on the Audit Commission's website at: <http://www.audit-commission.gov.uk/nfi/>

Appendix 3.

Extracts from statutory provisions

This appendix sets out extracts from the following statutory provisions:

1. Schedules 1 - 3 of the Data Protection Act 1998 – regarding fair processing requirements
2. Section 27 of the Data Protection Act 1998
3. Section 29 of the Data Protection Act 1998
4. Section 34 of the Data Protection Act 1998
5. Section 35 of the Data Protection Act 1998
6. Section 35 and 38 of the Freedom of Information (Scotland) Act 2002
7. Sections 26A-D of the Public Finance and Accountability (Scotland) Act 2000

1. Data protection principles and fair processing requirements in the Data Protection Act 1998

Schedule 1, Part I, - The Principles

- 1 Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless—
 - (a) at least one of the conditions in Schedule 2 is met, and
 - (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
- 2 Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
- 3 Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

- 4 Personal data shall be accurate and, where necessary, kept up to date.
- 5 Personal data processed for any purpose or purposes shall not be kept longer than is necessary for that purpose or those purposes.
- 6 Personal data shall be processed in accordance with the rights of data subjects under this Act.
- 7 Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- 8 *[text omitted from this extract]*

Schedule 1, Part II Interpretation of the Principles in Part I

The first principle

- 1
 - (1) In determining for the purposes of the first principle whether personal data are processed fairly, regard is to be had to the method by which they are obtained, including in particular whether any person from whom they are obtained is deceived or misled as to the purpose or purposes for which they are to be processed.
 - (2) Subject to paragraph 2, for the purposes of the first principle data are to be treated as obtained fairly if they consist of information obtained from a person who—
 - (a) is authorised by or under any enactment to supply it, or

- (b) is required to supply it by or under any enactment or by any convention or other instrument imposing an international obligation on the United Kingdom.

2

- (1) Subject to paragraph 3, for the purposes of the first principle personal data are not to be treated as processed fairly unless—
 - (a) in the case of data obtained from the data subject, the data controller ensures so far as practicable that the data subject has, is provided with, or has made readily available to him, the information specified in sub-paragraph (3), and
 - (b) in any other case, the data controller ensures so far as practicable that, before the relevant time or as soon as practicable after that time, the data subject has, is provided with, or has made readily available to him, the information specified in sub-paragraph (3).
- (2) In sub-paragraph (1)(b) “the relevant time” means—
 - (a) the time when the data controller first processes the data, or
 - (b) in a case where at that time disclosure to a third party within a reasonable period is envisaged—
 - i. if the data are in fact disclosed to such a person within that period, the time when the data are first disclosed,

<p>ii. if within that period the data controller becomes, or ought to become, aware that the data are unlikely to be disclosed to such a person within that period, the time when the data controller does become, or ought to become, so aware, or</p> <p>iii. in any other case, the end of that period.</p>	<p>(a) that the provision of that information would involve a disproportionate effort, or</p> <p>(b) that the recording of the information to be contained in the data by, or the disclosure of the data by, the data controller is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.</p>	<p>(b) for the exercise of any functions conferred on any person by or under any enactment,</p> <p>(c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or</p> <p>(d) for the exercise of any other functions of a public nature exercised in the public interest by any person.</p>
<p>(3) The information referred to in sub-paragraph (1) is as follows, namely—</p>	<p>4</p> <p><i>[text omitted from this extract]</i></p>	<p>6</p>
<p>(a) the identity of the data controller,</p> <p>(b) if he has nominated a representative for the purposes of this Act, the identity of that representative,</p> <p>(c) the purpose or purposes for which the data are intended to be processed, and</p> <p>(d) any further information which is necessary, having regard to the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair.</p>	<p>Schedule 2 Conditions Relevant for Purposes of the First Principle: Processing of any Personal Data</p> <p>1</p> <p><i>[text omitted from this extract]</i></p> <p>2</p> <p><i>[text omitted from this extract]</i></p> <p>3</p> <p>The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.</p>	<p>(1) The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.</p> <p>(2) The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.</p>
<p>3</p> <p>(1) Paragraph 2(1) (b) does not apply where either of the primary conditions in sub-paragraph (2), together with such further conditions as may be prescribed by the Secretary of State by order, are met.</p>	<p>4</p> <p><i>[text omitted from this extract]</i></p> <p>5</p> <p>The processing is necessary—</p>	<p>Schedule 3 Conditions Relevant for Purposes of the First Principle: Processing of Sensitive Personal Data</p> <p>1</p> <p><i>[text omitted from this extract]</i></p>
<p>(2) The primary conditions referred to in sub-paragraph (1) are—</p>	<p>(a) for the administration of justice,</p> <p>(aa) <i>[text omitted from this extract]</i></p>	<p>2</p> <p>(1) The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed</p>

by law on the data controller in connection with employment.

(2) *[text omitted from this extract]*

3 – 5

[text omitted from this extract]

6

The processing—

- (a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),
- (b) is necessary for the purpose of obtaining legal advice, or
- (c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

7

(1) The processing is necessary—

- (a) for the administration of justice,
- (aa) *[text omitted from this extract]*
- (b) for the exercise of any functions conferred on any person by or under an enactment, or
- (c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department.

(2) The Secretary of State may by order—

- (a) exclude the application of subparagraph (1) in such cases as may be specified, or

(b) provide that, in such cases as may be specified, the condition in subparagraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

8 – 10

[text omitted from this extract]

2. Relevant parts of Section 27 of the Data Protection Act 1998

Subject information and non-disclosures provisions

(1) *[text omitted from this extract]*

(2) In this Part “the subject information provisions” means—

- (a) the first data protection principle to the extent to which it requires compliance with paragraph 2 of Part II of Schedule 1, and

(b) section 7.

(3) In this Part “the non-disclosure provisions” means the provisions specified in subsection (4) to the extent to which they are inconsistent with the disclosure in question.

(4) The provisions referred to in subsection (3) are—

- (a) the first data protection principle, except to the extent to which it requires compliance with the conditions in Schedules 2 and 3,

(b) the second, third, fourth and fifth data protection principles, and

(c) sections 10 and 14(1) to (3).

(5) Except as provided by this Part, the subject information provisions shall have effect notwithstanding any enactment or rule of law prohibiting or restricting the disclosure, or authorising the withholding, of information.

3. Relevant parts of Section 29 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.

(2) *[text omitted from this extract]*

(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.

(4)-(5) *[text omitted from this extract]*

4. Section 34 of the Data Protection Act 1998

Section 34 Information available to the public by or under enactment

Personal data are exempt from-

- (a) the subject information provisions,
- (b) the fourth data protection principle and section 14(1) to (3), and
- (c) the non-disclosure provisions,

if the data consist of information which the data controller is obliged by or under any enactment, other than an enactment contained in the Freedom of Information Act 2000, to make available to the public, whether by publishing it, by making it available for inspection, or otherwise and whether gratuitously or on payment of a fee.

5. Relevant parts of Section 35 of the Data Protection Act 1998

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.

(2) *[text omitted from this extract]*

6. Relevant parts of Sections 35 and 38 of the Freedom of Information (Scotland) Act 2002

Section 35 Law enforcement

- (1) Information is exempt information if its disclosure under this Act would, or would be likely to, prejudice substantially -

(a) the prevention or detection of crime,

(b) the apprehension or prosecution of offenders,

(c) - (h) *[text omitted from this extract]*

(2) *[text omitted from this extract]*

Section 38 Personal information

- (1) Information is exempt information if it constitutes -

(a) personal data of which the applicant is the data subject;

(b) personal data and either the condition mentioned in subsection (2) (the "first condition") or that mentioned in subsection (3) (the "second condition") is satisfied.

(2) The first condition is-

(a) in a case where the information falls within any of paragraphs (a) to (d) of the definition of "data" in section 1(1) of the Data Protection Act 1998, that the disclosure of the information to a member of the public otherwise than under this Act would contravene-

(i) any of the data protection principles, or

(ii) section 10 of that Act (right to prevent processing likely to cause damage or distress), and

(b) in any other case, that the disclosure of the information to a member of the public otherwise than under this Act would contravene any of the data protection principles if the exemptions in section 33A(1) of the Data Protection Act 1998 (which relate to manual data held) were disregarded.

(3) The second condition is that by virtue of any provision of Part IV of the Data Protection Act 1998 the information is exempt from section 7(1)(c) of that Act (data subject's right of access to personal data).

(4) In determining for the purposes of this section whether anything done before 24th October 2007 would contravene any of the data protection principles, the exemptions in Part III of Schedule 8 to that Act are to be disregarded.

(5) In this section-

"the data protection principles" means the principles set out in Part I of Schedule 1 to the Data Protection Act 1998, as read subject to Part II of that Schedule and section 27(1) of that Act;

"data subject" and "personal data" have the meanings respectively assigned to those terms by section 1(1) of that Act;

7. Extracts from Sections 26A-D of the Public Finance and Accountability (Scotland) Act 2000 (as inserted by Section 97 of the Criminal Justice and Licensing (Scotland) Act 2010)

26A Power to carry out data matching exercises

- (1) Audit Scotland may carry out data matching exercises or arrange for them to be carried out on its behalf.
- (2) A data matching exercise is an exercise involving the comparison of sets of data to determine how far they match (including the identification of any patterns and trends).
- (3) The power in subsection (1) may be exercised for one or more of the following purposes—
 - (a) assisting in the prevention and detection of fraud,
 - (b) assisting in the prevention and detection of crime (other than fraud),
 - (c) assisting in the apprehension and prosecution of offenders.
- (4) A data matching exercise may not be used for the sole purpose of identifying patterns and trends in a person's characteristics or behaviour which suggest the person is likely to commit fraud in the future.

26B Voluntary disclosure of data to Audit Scotland

- (1) For the purposes of a data matching exercise, any person may disclose data to Audit

Scotland (or a person acting on its behalf).

- (2) Such disclosure does not breach—
 - (a) any duty of confidentiality owed by the person making the disclosure, or
 - (b) any other restriction on the disclosure of data.
- (3) Nothing in this section authorises a disclosure—
 - (a) which contravenes the Data Protection Act 1998 (c.29),
 - (b) which is prohibited by Part 1 of the Regulation of Investigatory Powers Act 2000 (c.23) (interception, acquisition and disclosure of communications data), or
 - (c) of data comprising or including patient data.
- (4) "Patient data" means data relating to an individual which is held for medical purposes and from which the individual can be identified.
- (5) "Medical purposes" are the purposes of—
 - (a) preventative medicine,
 - (b) medical diagnosis,
 - (c) medical research,
 - (d) the provision of care and treatment,
 - (e) the management of health and social care services, and
 - (f) informing individuals about their physical or mental health

or condition, the diagnosis of their condition or their care and treatment.

- (6) Nothing in this section prevents disclosure of data under any other provision of this Act, another enactment or any rule of law.
- (7) Data matching exercises may include data disclosed by a person outside Scotland.

26C Power to require disclosure of data

- (1) Audit Scotland may require the persons mentioned in subsection (2) to disclose to it (or a person acting on its behalf) such data as it (or the person acting on its behalf) may reasonably require for the purpose of carrying out data matching exercises.
- (2) Those persons are—
 - (a) a body or office holder any of whose accounts is an account in relation to which sections 21 and 22 apply,
 - (b) a body whose accounts must be audited under Part 7 of the Local Government (Scotland) Act 1973 (finance) (c.65),
 - (c) a licensing board continued in existence by or established under section 5 of the Licensing (Scotland) Act 2005 (asp 16), or
 - (d) an officer or member of a body, office holder or board mentioned in paragraph (a), (b) or (c).

- (3) Audit Scotland must not require a person to disclose data if—

- (a) the disclosure would contravene the Data Protection Act 1998 (c.29),
- (b) the disclosure is prohibited by Part 1 of the Regulation of Investigatory Powers Act 2000 (c.23) (interception, acquisition and disclosure of communications data).
- (4) A disclosure made in response to a requirement imposed under subsection (1) does not breach—
- (a) any duty of confidentiality owed by the person making the disclosure, or
- (b) any other restriction on the disclosure of data.
- (5) A person mentioned in subsection (2) who without reasonable excuse fails to comply with a requirement made in accordance with this section is guilty of an offence and liable on summary conviction to a fine not exceeding level 3 on the standard scale.
- 26D Disclosure of results of data matching**
- (1) This section applies to the following data—
- (a) data relating to a particular person obtained by or on behalf of Audit Scotland for the purpose of carrying out a data matching exercise, and
- (b) the results of such an exercise.
- (2) Data to which this section applies may be disclosed by or on behalf of Audit Scotland if the disclosure is—
- (a) for, or in connection with, a purpose for which a data matching exercise is carried out,
- (b) to a Scottish audit agency, or a related party, for, or in connection with a function of that audit agency under—
- (i) Part 2 of this Act, or
- (ii) Part 7 of the Local Government (Scotland) Act 1973 (c.65) (finance),
- (c) to a United Kingdom audit agency, or a related party, for, or in connection with, a function of that audit agency corresponding or similar to—
- (i) the functions of a Scottish audit agency, or
- (ii) the functions of Audit Scotland under this Part, or
- (d) in pursuance of a duty imposed by or under an enactment.
- (3) “Scottish audit agency”, for the purpose of subsections (2)(b) and (2)(c)(i), means—
- (a) the Auditor General, or
- (b) the Accounts Commission.
- (4) “United Kingdom audit agency”, for the purposes of subsection (2)(c), means—
- (a) the National Audit Office,
- (b) the Audit Commission for Local Authorities and the National Health Service in England,
- (c) the Auditor General for Wales,
- (d) the Comptroller and Auditor General for Northern Ireland, or
- (e) a person designated as a local government auditor under article 4 of the Local Government (Northern Ireland) Order 2005 (S.I. 2005/1968 (NI.18)).
- (5)-(7) *[text omitted from this extract]*
- (8) Data disclosed under subsection (2) may not be further disclosed except—
- (a) for, or in connection with—
- (i) the purpose for which it was disclosed under subsection (2)(a), or
- (ii) the function for which it was disclosed under subsection (2)(b) or (c),
- (b) otherwise for the investigation or prosecution of an offence, or
- (c) in pursuance of a duty imposed by or under an enactment.
- (9) Except as authorised by subsections (2) and (8), a person who discloses data to which this section applies is guilty of an offence and liable—
- (a) on summary conviction, to imprisonment for a term not exceeding 12 months, to a fine or to both, or
- (b) on conviction on indictment, to imprisonment for a term not exceeding two years, to a fine or to both.

Code of data matching practice 2010

Issued under Section 26F of the Public Finance and
Accountability (Scotland) Act 2000 (as amended)

If you require this publication in an alternative format
and/or language, please contact us to discuss your needs.

You can also download this document at:
www.audit-scotland.gov.uk



Audit Scotland, 110 George Street, Edinburgh EH2 4LH
T: 0845 146 1010 E: info@audit-scotland.gov.uk
www.audit-scotland.gov.uk