



23 September 2008
www.wao.gov.uk

WALES **AUDIT** OFFICE
SWYDDFA **ARCHWILIO** CYMRU

The Code of Data Matching Practice of the Auditor General for Wales

The Code of Data Matching Practice of the Auditor General for Wales

I have prepared this Code of Data Matching Practice, following a statutory consultation process, for presentation to the National Assembly under the Public Audit (Wales) Act 2004.

Jeremy Colman
Auditor General for Wales
Wales Audit Office
24 Cathedral Road
Cardiff
CF11 9LJ

The Auditor General is totally independent of the National Assembly and Government. He examines and certifies the accounts of the Assembly Government and its sponsored and related public bodies, including NHS bodies in Wales. He also has the statutory power to report to the National Assembly on the economy, efficiency and effectiveness with which those organisations have used, and may improve the use of, their resources in discharging their functions.

The Auditor General also appoints auditors to local government bodies in Wales, conducts and promotes value for money studies in the local government sector and inspects for compliance with best value requirements under the Wales Programme for Improvement. However, in order to protect the constitutional position of local government, he does not report to the National Assembly specifically on such local government work, except where required to do so by statute.

The Auditor General and his staff together comprise the Wales Audit Office. For further information about the Wales Audit Office please write to the Auditor General at the address above, telephone 029 2032 0500, email: wales@wao.gov.uk, or see web site <http://www.wao.gov.uk>

© Auditor General for Wales 2008

You may re-use this publication (not including logos) free of charge in any format or medium. You must re-use it accurately and not in a misleading context. The material must be acknowledged as Auditor General for Wales copyright and you must give the title of this publication.

**Presented by the Auditor General for Wales to the National
Assembly for Wales on 23 September 2008**

	Foreword by the Auditor General for Wales	6
	Foreword by the Information Commissioner	7
1	The Auditor General undertakes data matching to help prevent and detect fraud, and has prepared this Code to guide all who participate in such work	8
	Data matching is the comparison of information, such as payroll, from a variety of sources in order to identify fraud, and so improve value-for-money	8
	The Auditor General does data matching under a statutory framework, and this Code is a statutory requirement	8
	The Code is to help all bodies involved in data matching to comply with the law and good practice, and it is to inform individuals about the data matching process	10
	Local government and NHS bodies may be required to provide personal data of their employees, members and people they serve for matching, and other bodies may also participate	10
	The Auditor General requires each Participating Body to nominate suitably senior members of staff to be responsible for data matching exercises and provides handbooks for guidance	11
	The Auditor General will only undertake data matching where there is an appreciable risk of fraud	12
2	Fairness and transparency: Participating Bodies must let people know about the use of their data for matching, unless an exemption applies	13
	The Information Commissioner recommends layered fair processing notices	13
	Participating Bodies should provide summary fair processing notices when collecting new personal data, or retrospective notices where this opportunity has passed	14
	Participating Bodies should be careful in dealing with data relating to deceased persons	15

	Participating Bodies must register for prevention and detection of fraud processing purposes with the Information Commissioner’s Office	15
	The Auditor General will also provide information about his data matching exercises	15
3	Information Standards: Participating Bodies should ensure that the personal data they supply are of sufficient quality	16
4	Security: Participating Bodies and the Auditor General must protect the personal data and related information involved	17
	The Auditor General will ensure that data matching is done fairly and only for the purpose of assisting in the prevention and detection of fraud	18
	The Auditor General will ensure that data matching output is disseminated securely	18
	The disclosure of data used in data matching is strictly controlled	18
5	Retention: the data will be held for no longer than is necessary	20
6	Access to personal data and information about the details of data matching exercises will be restricted	21
7	Review: The Auditor General will keep data matching procedures under review and invite the Information Commissioner to assess compliance	22
Appendices		
	Appendix 1 - Definitions of terms used in the Code	23
	Appendix 2 - Examples of good practice layered fair processing notices	24
	Appendix 3 - Relevant statutory provisions	29
	Appendix 4 - Contact details	38

Foreword by the Auditor General for Wales

I am pleased to present this Code of Data Matching Practice to the National Assembly for Wales in accordance with the Public Audit (Wales) Act 2004.

The Serious Crime Act 2007 has amended the Public Audit (Wales) Act 2004, so as to give me new powers to undertake data matching exercises. The preparation of this Code, following consultation, and the observance of it by all participants in data matching exercises done under this legislation, are statutory requirements.

Data matching can be a powerful way of identifying fraud and overpayment. For example, my work with the Audit Commission and public sector bodies in Wales on the 2006/2007 National Fraud Initiative (NFI) identified £4.5 million of fraud and overpayment in Wales. But such work needs to be done carefully so as to prevent unnecessary intrusion into people's affairs.

This Code therefore promotes compliance with the law and good practice on the part of all participants in data matching exercises done using my powers. I have developed it taking account of responses to the statutory consultation and the Information Commissioner's Information Sharing Framework Code of Practice. It will help to ensure that people's information is protected and processed appropriately during data matching exercises. It also helps let individuals know why their data are matched, the standards and protections that apply and where to find further information.



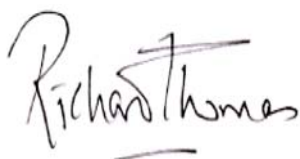
Jeremy Colman
Auditor General for Wales

Foreword by the Information Commissioner

The need to safeguard public funds from those who seek to make fraudulent claims continues to be a public concern. The National Fraud Initiative has shown that data matching exercises go some way towards identifying the fraudulent claims, preventing overpayments, and enabling bodies participating in the exercises to address these issues on the ground. However, the collation and use of large quantities of personal information in this way continues to raise substantial data protection risks. Often personal information used in such exercises will not be implicated in any fraudulent activity, and it is essential that auditors and the bodies participating in data matching exercises take their obligations under the Data Protection Act seriously.

The Auditor General for Wales, Audit Commission and the Northern Ireland Audit Office have involved the ICO in developing their Codes of Data Matching Practice. They have undertaken work to clarify the framework of rules and practices designed to protect personal information in these data matching exercises. We particularly welcome their efforts to clarify the lawful basis for these exercises, the importance of transparency and the need for effective security as the exercises are expanded. This helps to address legitimate concerns that potentially intrusive exercises are carried out in a proportionate, lawful and secure manner. We have also begun auditing the data processing undertaken as part of the National Fraud Initiative and we will continue to take this forward during the course of the year.

The importance of protecting personal information has never been so prominent and it is essential that this Code is followed in practice in order for it to be truly effective. Compliance with this Code should enable the continued identification of those individuals involved in fraudulent activity and, significantly, it should preserve and protect the rights of the majority who are not.

A handwritten signature in black ink that reads "Richard Thomas". The signature is written in a cursive style with a horizontal line underneath the name.

Richard Thomas
Information Commissioner

Part 1 - The Auditor General undertakes data matching to help prevent and detect fraud, and has prepared this Code to guide all who participate in such work

1.1 The Auditor General is the external auditor of the Welsh public sector. He examines and certifies the accounts of the Welsh Assembly Government and its sponsored and related public bodies, including NHS bodies in Wales. He has the statutory power to report to the National Assembly for Wales (the National Assembly) on the economy, efficiency and effectiveness with which those organisations have used, and may improve the use of, their resources in discharging their functions. He also appoints auditors to local government bodies in Wales and conducts and promotes value-for-money studies in the local government sector.

Data matching is the comparison of information, such as payroll, from a variety of sources in order to identify fraud, and so improve value-for-money

1.2 It is important 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 the Auditor General and the local government auditors that he appoints.

1.3 Data matching exercises, such as the National Fraud Initiative (NFI) that the Auditor General does in co-operation with the Audit Commission (and in future other UK audit bodies), help audited bodies to prevent and detect fraud and error, so securing better

value from public money. The exercises also help the Auditor General and his auditors to assess the arrangements that audited bodies have put in place to deal with fraud, which can help the bodies to achieve further improvements.

1.4 Data matching involves comparing sets of data, such as the payroll or benefits records of one body against other records held by the same or another body. This allows fraudulent claims and payments to be identified. Where a match is found, it may indicate that there is an inconsistency which requires further investigation; it is not necessarily evidence of fraud. Where no match is found, the data matching powers will have no material effect on those concerned. In the NFI, for example, participating bodies have received a report of matches that they should investigate, so as to detect instances of fraud and error, and take remedial action.

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

The Auditor General does data matching under a statutory framework, and this Code is a statutory requirement

1.6 From 2008, the Auditor General will conduct data matching exercises under his new statutory powers contained in the Public Audit (Wales) Act 2004 (the 2004 Act), as amended by the Serious Crime Act 2007 (key sections

are set out in Appendix 3). Previous exercises were undertaken under value-for-money examination and study functions in the 2004 Act and the Government of Wales Act 1998, and under appointed auditor's powers. Under the new legislation:

- a** the Auditor General may carry out data matching exercises for the purpose of assisting in the prevention and detection of fraud, as part of an audit or otherwise;
- b** the Auditor General may require local government and NHS bodies in Wales to provide data for data matching exercises;
- c** other bodies may participate in his data matching exercises on a voluntary basis where the Auditor General considers it appropriate. Where they do so, the statute states that there is no breach of confidentiality or, with certain exceptions (see section 64C of the 2004 Act in Appendix 3), any other restriction in providing the data to the Auditor General;
- d** the requirements of the Data Protection Act 1998 continue to apply;
- e** the Auditor General may disclose the results of data matching exercises to bodies that have provided the data and to auditors that he appoints;
- f** the Auditor General may publish a summary report;
- g** the Auditor General may disclose both data provided for data matching and the results of data matching to the Audit Commission, the Comptroller and Auditor General for Northern Ireland, the Auditor General for Scotland, the Accounts Commission for Scotland and Audit Scotland for the

purposes of preventing and detecting fraud;

- h** wrongful disclosure of data obtained for the purposes of data matching by any person is a criminal offence;
- i** the Auditor General may charge a fee to any body participating in a data matching exercise and must set a scale of fees for bodies required to participate; and
- j** the Auditor General must prepare a Code of Practice following consultation with bodies required to participate (local government and NHS), the Information Commissioner and other bodies that the Auditor General thinks fit. He must also lay a copy of the Code and any alterations made to it before the National Assembly, and publish the Code. All bodies conducting or participating in his data matching exercises must have regard to the Code, including the Auditor General himself.

1.7 The Auditor General may conduct data matching exercises himself, or arrange for them to be done for him. In practice, most of the Auditor General's data matching will be done in the form of joint exercises with other UK audit agencies, such as the National Fraud Initiative. In this, the Audit Commission has undertaken all the key aspects of the exercise for the Auditor General¹ and other UK auditors, including the collection and processing of data.

1.8 As set out at 1.6(j) above, this Code is a statutory requirement. It will govern all the Auditor General's future data matching exercises for the purposes of the prevention and detection of fraud until a replacement is laid before the National Assembly. The Auditor

¹ The Auditor General has the power to obtain such services as the Auditor General considers necessary for assisting in the Auditor General's functions under paragraph 7 of Schedule 8 of the Government of Wales Act 2006. The Auditor General also has to power under paragraph 21 of the 2006 Act to make arrangements to co-operate with other public bodies to facilitate the exercise of the Auditor General's and other bodies' functions.

General intends to review and update the Code periodically in the light of changes in the law and to reflect comments and experience drawn from each data matching exercise.

- 1.9** Any person or body conducting, or participating, in any of the Auditor General's data matching exercises must, by law, have regard to the provisions of this Code. They should also have regard to any other relevant information sharing codes and policies. Any questions about this Code or particular data matching exercises should be addressed to the NFI Co-ordinator, Wales Audit Office, 24 Cathedral Road, Cardiff, CF11 9LJ (nfi@wao.gov.uk). Complaints about bodies participating in the Auditor General's data matching exercises should be addressed to those bodies. Complaints about the Auditor General's role, or that of his staff or appointed auditors, in conducting data matching exercises should be made to the Wales Audit Office Complaints Manager so that they can be dealt with under the Wales Audit Office complaints procedure. Further information and contact details are at Appendix 4.

The Code is to help all bodies involved in data matching to comply with the law and good practice, and it is to inform individuals about the data matching process

- 1.10** The purpose of this Code is to help ensure that the Auditor General and his staff, the auditors that the Auditor General appoints and all bodies involved in data matching exercises comply with the law, especially the provisions

of the Data Protection Act 1998. It is also intended to promote good practice in data matching and to let individuals know why their data is matched and by whom, the standards which apply and where to find further information. Certain terms (identified by initial capitals) used in this Code are defined at Appendix 1.

- 1.11** This Code does not, however, strictly apply to the detailed steps taken by a Participating Body to investigate matches from a data matching exercise. It is for Participating Bodies to investigate matches in accordance with their usual practices for investigation of fraud and error.

Local government and NHS bodies may be required to provide personal data of their employees, members and people they serve for matching, and other bodies may also participate

- 1.12** Under the Public Audit (Wales) Act 2004 (as amended by the Serious Crime Act 2007), the Auditor General may require all local government bodies and NHS bodies in Wales to provide personal data relating to their employees, members and the people they serve for data matching exercises. Bodies required to participate in this way are referred to in this Code as Mandatory Bodies. Mandatory Bodies must provide data for data matching exercises as required by the Auditor General under section 64B of the 2004 Act. Failure to provide data as required without reasonable excuse is a criminal offence (section 64B(3)—see Appendix 3).

1.13 Any other body or person may provide data voluntarily for data matching exercises if the Auditor General decides that it is appropriate to use their data. These are referred to as Voluntary Participating Bodies in this Code. Where a Voluntary Participating Body provides data to the Auditor General for data matching, the law (section 64C of the 2004 Act) provides that this does not amount to a breach of confidentiality, and generally does not breach other legal restrictions. However, Patient Data may not be shared voluntarily, and so may only be used in data matching if the Auditor General requires it from a Mandatory Body.

1.14 Whether a Participating Body provides 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. In practice, this will mean that the disclosure of data is either in accordance with the data protection principles, or a relevant exemption within the Data Protection Act has been applied. In most cases, data matching will be done in accordance with the data protection principles without reliance on exemptions provided by the Data Protection Act. The main exemptions in relation to obtaining and providing data are sections 34 and 35 of the Data Protection Act. These need to be considered in the circumstances of each data matching exercise. Relevant extracts from the Data Protection Act, including the data protection principles, are set out in Appendix 3.

The Auditor General requires each Participating Body to nominate suitably senior members of staff to be responsible for data matching exercises and provides handbooks for guidance

1.15 The Auditor General requires each Participating Body's Director of Finance or equivalent to be the Responsible Officer and to nominate a suitably senior member of staff to be the Key Contact for each data matching exercise. The Responsible Officer should also nominate suitable staff to be responsible for data handling and the follow-up investigation of matches. The Responsible Officer should ensure that nominated staff are suitably qualified and trained for their role.

1.16 The Key Contact should liaise with the Data Protection Officer for the Participating Body. The Data Protection Officer should be involved in the arrangements for data handling, training and providing Fair Processing Notices at an early stage.

1.17 The NFI Co-ordinator is the principal point of contact at the Wales Audit Office for the Auditor General's data matching exercises (nfi@wao.gov.uk). Full contact details are at Appendix 4.

1.18 For each data matching exercise, the Auditor General (or his agent) will make guidance available to all Participating Bodies. This will set out the detailed responsibilities and requirements for participation. The most up-to-date guidance may be found at <http://www.wao.gov.uk/whatwedo/1252.asp>. The guidance will contain:

- a a list of the responsibilities of the nominated officers at the Participating Body;
- b specifications for each set of data (listing the minimum data to be provided by the Participating Body to enable data matching and to ensure results of sufficient quality);
- c details of any further requirements and returns concerning the data to be provided;
- d a timetable for processing;
- e a data protection compliance return; and
- f information on how to interpret matches, and on co-operation between participating bodies.

The Auditor General will only undertake data matching where there is an appreciable risk of fraud

- 1.19** The Auditor General will only choose sets of data for matching where there is reasonable evidence that fraud is likely to be found as a result. This will be the key consideration when the Auditor General decides whether it is appropriate to accept data from a Voluntary Participating Body, or to require data from a Mandatory Body. Evidence may come from previous data matching exercises, from pilot exercises, from Participating Bodies or from other reliable sources of information, such as auditors appointed by the Auditor General.
- 1.20** The Auditor General will undertake new areas of data matching on a pilot basis to test their effectiveness in preventing or detecting fraud. Only where pilots achieve matches that demonstrate a significant level of potential

fraud will they be extended nationally. A significant level may be indicated by a few serious incidents of fraud or a larger number of smaller ones. 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. The Auditor General will also review the results of each full data matching exercise in order to refine how he chooses data for future exercises.

- 1.21** The data required from Participating Bodies 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 Auditor General's guidance for each exercise. Any revisions to the data specifications will generally be published at least six months before the data sets are to be provided on the Wales Audit Office website at <http://www.wao.gov.uk/whatwedo/1252.asp>. The Auditor General's NFI Co-ordinator will draw the attention of Participating Bodies' Key Contacts to such revisions by email. This is to ensure that Participating Bodies have early notification of any changes so they can prepare adequately.
- 1.22** The selection processes will minimise the risk that large amounts of personal data are processed without any significant risk of fraud being present. However, it is necessary in order for fraud to be detected for the personal data of individuals who have no involvement in fraud whatsoever to be processed. But unless there are anomalies that lead to subsequent investigation, people whose data are subject to data matching will not be affected by the processing in any material sense.

Part 2 - Fairness and transparency: Participating Bodies must let people know about the use of their data for matching, unless an exemption applies

- 2.1** The processing of data by the Auditor General in a data matching exercise is carried out with statutory authority. Under the Data Protection Act 1998, it does not therefore require the consent of the individuals concerned. The relevant provisions of the Data Protection Act are in Appendix 3.
- 2.2** Participating Bodies, both Mandatory and Voluntary, should notify individuals that their data will be processed, as required by the Data Protection Act 1998. Unless an exemption applies, for data processing to be fair, data controllers must 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; and
 - c** any further information which is necessary to enable the processing to be fair.
- 2.3** This information is provided in writing using fair processing notices. These enable people to know that their data are being used in order to prevent or detect fraud and to take appropriate steps if they consider the use is unjustified or unlawful in their particular case.
- 2.4** Participating Bodies should, so far as practicable, ensure notices are actively provided, or at least made readily available, to the individuals that they are sharing information about. The notice should clearly set out an explanation that that their data may be disclosed for the purpose of preventing and detecting fraud. They should also give notice that the data will be provided to the Auditor General for this purpose. The notice should also contain details of how individuals can find out more information about the processing.
- 2.5** 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.
- 2.6** When providing data to the Auditor General, or for the NFI, to the Audit Commission as the Auditor General's agent, the Participating Body should submit a declaration confirming compliance with the fair processing notification requirements. The Auditor General will check that the requirements have been adhered to and, where necessary, will agree the steps necessary for the Participating Body to achieve compliance. He will also seek input from the Information Commissioner as part of this process.

The Information Commissioner recommends layered fair processing notices

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

2.8 The *summary notice* should provide the minimum necessary content and should be provided to the individuals whose data are 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 the Key Contact or Information Officer. Participating Bodies should make clear where individuals can obtain further information about how, why and by whom their data is being processed.

2.9 In the case of benefits, licences and applications for services, for example, the summary notice should be included on the application form used to collect the data in the first place. In other cases, such as occupational pensioners, where Participating Bodies usually communicate once a year using, for example, a newsletter, summary notices should be included in these communications in advance of each exercise. This will avoid the cost of a separate mailing.

2.10 Participating Bodies should notify their employees on recruitment, such as by including a summary notice in appointment letters. They should also provide a summary notice before each exercise, for example, by including this in their payslips.

2.11 The *condensed text* should give a summary of the Auditor General's data matching exercises, and should be available on the Participating Body's website and in hard copy on request. This layer should provide a link to the more detailed full text.

2.12 The *full text* will be available on the Auditor General's website and will include an explanation of the legal basis for its data matching exercises and a more detailed description of how the initiative works.

2.13 While Participating Bodies should decide the content and means of issue of fair processing notices for themselves, good practice examples of a three-layered approach are included at Appendix 2. The Auditor General's NFI Co-ordinator will also draw the attention of Participating Bodies' Key Contacts for each exercise to these examples, and any revisions to them, by email. Such notices will have the effect of deterring fraud as well as informing applicants about the use of data in data matching. If Participating Bodies or the Auditor General fall short of good practice, the Information Commissioner may investigate and take enforcement action. The Information Commissioner's contact details are at 7.4.

2.14 The benefit of using a layered approach is to give appropriate levels of fair processing 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, and more comprehensive information can be made available for others.

Participating Bodies should provide summary fair processing notices when collecting new personal data, or retrospective notices where this opportunity has passed

2.15 Participating Bodies should, where practicable, provide summary fair processing notices at the point of collecting personal data. Participating Bodies should in any event provide such notices before disclosing the data to the Auditor General or his agents, unless it is impracticable to do so.

2.16 Sometimes it will not be practicable to provide a summary fair processing notice at the time of the original collection of the data. In such cases, Participating Bodies should provide retrospective summary fair processing notices at the earliest reasonable opportunity, and before disclosure to the Auditor General or his agent, unless it is impracticable to do so.

Participating Bodies should be careful in dealing with data relating to deceased persons

2.17 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 any case, so as not to cause any unnecessary distress or harm, 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.

Participating Bodies must register for prevention and detection of fraud processing purposes with the Information Commissioner's Office

2.18 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 the 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 are processed and specified information in relation to each purpose. Those data controllers that are required to notify, but fail to do so, commit a criminal offence. It is the responsibility of all Participants (both Mandatory and Voluntary) to ensure their notification to the Information Commissioner covers the Auditor General and auditors as recipients against the appropriate purposes: the prevention and detection of fraud.

2.19 A Notification Handbook is available from the Information Commissioner's Office, 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.

The Auditor General will also provide information about his data matching exercises

2.20 To complement the information provided by fair processing notices, the Auditor General will from time to time publicise the fact that he undertakes data matching exercises and the reasons for them, such as when new exercises commence. This will include the provision of summary leaflets for distribution and audio equivalents.

Part 3 - Information Standards: Participating Bodies should ensure that the personal data they supply are of sufficient quality

- 3.1** Participating Bodies should ensure that the data they provide to the Auditor General and his agents are of good quality in terms of accuracy and completeness. Processing inaccurate data will mean that the Participating Body is in breach of the Data Protection Act. Therefore, before providing personal data for matching, bodies should ensure that these are as accurate and up to date as possible. Errors identified from previous data matching exercises should be rectified, and action taken to address issues raised in data quality reports supplied from those exercises.
- 3.2** The Participating Body's Responsible Officer should ensure that all requests from people whose data are to be matched for their data to be updated or corrected have been processed. Where Participating Bodies find that any such requests are outstanding, they must carefully note the requests and ensure that they are taken into account when referring to match reports.

Part 4 - Security: Participating Bodies and the Auditor General must protect the personal data and related information involved

- 4.1** Security arrangements for handling and storage of data by all participating in data matching exercises, including the Auditor General and any firm or body undertaking data matching as his agent, should ensure that:
- a** specific responsibility for security of data has been allocated to one or more managers;
 - b** security measures take appropriate account of the physical environment in which data are held, including the security of premises and storage facilities;
 - c** there are physical and logical controls to restrict access to electronic data so that only those who need to access the data for the purpose of a data matching exercise 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;
 - e** there are robust mechanisms in place for recording access, use and transfer of data; and
 - f** if 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. The responsible body should also follow the Information Commissioner's guidance on the management of security breaches. Participating Bodies' key contacts and the Wales Audit Office NFI Co-ordinator (nfi@wao.gov.uk) should inform one another immediately in the event of a confirmed security breach.
- 4.2** All persons handling data as part of the data matching exercise should be made aware of their data protection, confidentiality and security obligations under the Data Protection Act 1998, the 2004 Act and this Code. They 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.
- 4.3** Where the Auditor General or his agents establish websites for the transmission of data or the results of data matching, these will be password protected and encrypted to 128 bit SSL standards. This applies to the current NFI website established by the Audit Commission.
- 4.4** Any body or firm processing data as the Auditor General's agents will do so under a written agreement or contract that requires the agent's technical and organisational security standards to meet ISO 27001/02. The Auditor General will obtain assurance on compliance with these standards from time to time.
- 4.5** Participating Bodies should make all reasonable efforts to ensure the security of data in transmission to the Auditor General or his agents. For the NFI, they should only despatch data to the Audit Commission using the secure NFI website. For other exercises, data should only be provided to Wales Audit Office staff in person who will ensure its

secure transit, including encryption to relevant standards. Participating Bodies and appointed auditors should also ensure the security of data transmission within their own organisations.

The Auditor General will ensure that data matching is done fairly and only for the purpose of assisting in the prevention and detection of fraud

- 4.6** The Auditor General will ensure that data matching is done fairly and for the purpose of assisting in the prevention and detection of fraud. The techniques used by the Auditor General or his agents in data matching exercises will only be those that can reasonably indicate potential fraud. They will be refined in the light of practical experience, having identified any lessons from reviewing the results of previous exercises.
- 4.7** All data transmitted and stored electronically by the Auditor General or his agents will be held on a secure, password-protected computer system maintained in a secure environment. All staff of the Auditor General and his agents who have access to personal data included in a data matching exercise will be subject to security clearance procedures.
- 4.8** All data provided for the purpose of data matching exercises will be backed up by the Auditor General or his agents at appropriate intervals, depending on the scale and duration of the exercise, 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.

The Auditor General will ensure that data matching output is disseminated securely

- 4.9** All results from data matching exercises, such as matches and other relevant information arising from processing, will be disclosed to Participating Bodies via secure web-access or by secure encrypted storage carried by Wales Audit Office staff.
- 4.10** The Responsible Officer should ensure that the results of a data matching exercise are disclosed only to named staff for each type of result. In the case of the NFI, the secure NFI website is designed for that purpose.
- 4.11** All results from data matching exercises held by the Participating Body should be password protected on a secure, password-protected computer system. Any printed results should be kept in locked storage in a secure environment and should only be accessible to named authorised individuals.

The disclosure of data used in data matching is strictly controlled

- 4.12** 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 the Auditor General for the purposes of data matching exercises and the results of the data matching.
- 4.13** There is legal authority to disclose the data or results when this will assist in the prevention and detection of fraud. This includes, for example, disclosure of the results to the Participating Body to investigate any matches and disclosure to an auditor appointed by the

Auditor General to enable them to assess the Participating Body's arrangements for the prevention and detection of fraud. However, patient data may only be shared for a purpose relating to a relevant NHS body.

- 4.14** The Auditor General may also disclose data to equivalent audit bodies in England, Northern Ireland and Scotland, to the bodies whose accounts they audit or arrange to be audited, and to the auditors they appoint. A body in receipt of results from the Auditor General or his agent may only disclose them further if it is to assist in the prevention and detection of fraud, to investigate and prosecute an offence, for the purpose of disclosure to an auditor or otherwise as required by statute.
- 4.15** The Auditor General may publish reports on his data matching exercises. These will summarise the work and the results achieved. They will not, however, include any personal 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. The Auditor General may report on the progress of prosecutions resulting from data matching as these will be in the public domain.
- 4.16** Any disclosure by the Auditor General, a Participating Body or any other person in breach of these restrictions is a criminal offence. The text of the relevant provision (section 64D of the Public Audit (Wales) Act 2004) is set out at Appendix 3.

Part 5 - Retention: the data will be held for no longer than is necessary

- 5.1** Participating Bodies should discuss with their audit engagement partner what should be retained in their individual circumstances, particularly with regard to records of matches that indicate fraud. They may, for example, be needed as working papers for the purposes of audit, or for the purpose of continuing investigation or prosecution.
- 5.2** The Auditor General or his agents will destroy all original data sets provided to him by participating bodies within six months of their submission. Particular data may need to be retained so as to provide evidence for prosecutions or for the qualification of accounts. The Auditor General will destroy all data derived or produced from the original data sets promptly and, with the exception of prosecution, money laundering reporting or qualification evidence, within three months of the conclusion of the exercise.
- 5.3** A single set of reference codes for matches will also be retained securely offline by the Auditor General or his agents for as long as they are relevant. This is solely for the purpose of preventing unnecessary reinvestigation of matches in any subsequent data matching exercise. Data retained will be subject to the requirements of the Data Protection Act.

Part 6 - Access to personal data and information about the details of data matching exercises will be restricted

- 6.1** Individuals whose data are included in a data matching exercise have rights of access to their information, and for ensuring its accuracy, under the Data Protection Act 1998. There are also rights to other information under the Freedom of Information Act 2000. Requests for information should be dealt with in accordance with the organisation's general arrangements for responding to requests for information.
- 6.2** However, personal data processed for the purposes of preventing and detecting fraud, as is the case with that used in data matching, may in particular circumstances be exempt from the subject access provisions of the Data Protection Act by virtue of section 29 of that Act (crime and taxation). This means that people may be refused access to their information processed in data matching exercises. However, this exemption would only relate to circumstances where disclosure would be likely to prejudice the prevention or detection of a crime or the apprehension or prosecution of an offender. This determination would be made on case-by-case basis. Personal information will normally fall within the personal information exemption (section 40) of the Freedom of Information Act, so preventing disclosure to other people.
- 6.3** 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 at <http://www.wao.gov.uk/whatwedo/1252.asp> or by contacting the Wales Audit Office's NFI Co-ordinator (see Appendix 4 for contact details). They should be able to check the accuracy of the data held on them by approaching the participating body holding the data.
- 6.4** Requests for other (non-personal) information under the Freedom of Information Act 2000, relating to data matching exercises, may be subject to the exemptions provided by the Freedom of Information Act, especially the law enforcement exemption (section 31). However, the law enforcement exemption would only relate to circumstances where disclosure would be likely to prejudice the prevention or detection of crime. This determination would be made on case by case basis. The Auditor General will, however, make information that is not covered by exemptions readily available through, for example, his published summary reports on data matching exercises. He will also regularly update his publication scheme to list materials that provide information about data matching exercises.
- 6.5** Participating Bodies should have procedures in place for dealing with requests from individuals for access to their data, and for complaints about the inclusion of their data in a data matching exercise. They should also have arrangements in place, as set out in paragraph 3.2, for updating and correcting data. If a Participating Body receives a complaint during a data matching exercise that concerns the statutory basis of the exercise, or the Auditor General is otherwise best placed to deal it, the Body should pass on the request promptly. Complaints about the Auditor General's role in conducting data matching exercises should be sent to the Wales Audit Office Complaints Manager (see Appendix 4) so that they can be dealt with under the Wales Audit Office complaints procedure.

Part 7 - Review: The Auditor General will keep data matching procedures under review and invite the Information Commissioner to assess compliance

7.1 The Auditor General will keep data matching procedures under review, such as in relation to whether:

- a** fair processing notices provided by Participating Bodies are adequate;
- b** the quality of data sets is acceptable;
- c** participants are meeting security standards; and
- d** participants are adhering to retention periods.

The Auditor General will also review the results of each exercise in order to refine the choice of data and the techniques used in future exercises. As part of his reviews, the Auditor General will consider any complaints from Participating Bodies or people whose data have been processed in the exercises.

7.2 Where the Auditor General becomes aware that a Participating Body has not complied with the requirements of the Code, he will notify the body concerned and seek to ensure that it puts in place adequate measures to meet the Code's requirements.

Questions regarding the Code and concerns regarding non-compliance should be made to the Participating Body or the Auditor General in the first instance.

7.3 Questions regarding the law and information sharing may be addressed to the Information Commissioner. The Information Commissioner regulates compliance with the Data Protection Act 1998. If a matter is referred to the Information Commissioner, he would consider compliance with this Code by

participant bodies and the Auditor General in determining the nature of any enforcement action. Guidance on the Information Commissioner's approach to enforcement and his Data Protection Strategy is available on his website.

7.4 The Commissioner may be contacted 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 on-line enquiries form for questions regarding the legislation for which the Information Commissioner is responsible)

7.5 The Information Commissioner has been invited (under section 51(7) of the Data Protection Act 1998) to review the Auditor General's data matching processing from time to time, to assess compliance with the Data Protection Act 1998. Participating Bodies are encouraged to invite the Information Commissioner's Office to review their procedures. The purpose of this review would be to assess Participating Bodies' 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
Code	Code of Data Matching Practice 2008
Data Matching	the comparison of sets of data, such as the payroll or benefits records of one body against other records held by the same or another body, to determine how far they match so as to allow inconsistencies that may be fraudulent claims and payments to be identified
Key Contact	the officer nominated by a Participating Body's Senior Responsible Officer to act as point of contact with the Auditor General and his agents (such as the Audit Commission) for the purposes of data matching exercises
Mandatory Body	a body that is required by the Auditor General pursuant to section 64B of the Public Audit (Wales) Act 2004 to provide data for a data matching exercise
Patient Data	data relating to an individual which are held for medical purposes (within the meaning of section 251 of the National Health Service Act 2006) and from which the individual can be identified--this includes both clinical data, such as medical records, and demographic data, such as the addresses of patients
Responsible Officer	the Director of Finance or other senior named member of staff of the Participating Body responsible for ensuring compliance with this Code
Participating Body	either a Mandatory or Voluntary Participating Body which provides data to the Auditor General or his agents (such as the Audit Commission) for the purposes of a data matching exercise
Voluntary Participating Body	a body from which the Auditor General considers it appropriate to accept data on a voluntary basis for the purpose of data matching

Appendix 2 – Examples of good practice layered fair processing notices

The Information Commissioner recommends that a layered approach is adopted when issuing fair processing notices. The purpose of each layer and the benefits of the approach are described in paragraphs 2.7 to 2.13.

Bodies participating in the Auditor General's data matching exercises must decide for themselves the content and means of issue of fair processing notices, but good practice examples are set out below. Bodies 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)

As a public body, we are under a duty to protect the public funds that we administer, and to this end may use the information you have provided on this form for the prevention and detection of fraud. We 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 authority's website} or contact {name and contact details}.

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 body's website} or contact {name and contact details}.

Level 1 – Summary Text – Example for Letters (for example, to pensioners, employees and tenants, where a newsletter, payslip or other standing form of communication is not available)

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

I am writing to let you know that {name of audited body} is participating in an exercise to ensure that public money is being spent properly.

The {name of audited body} 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.

The Auditor General currently requires us to participate in his anti-fraud data matching exercise. For this, we are providing details of [pensioners] for the purposes of comparing these with information provided by other public bodies. This will ensure 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 ensure 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]. However, if you do have any questions, you should contact {name and contact details}. Further information is also available on our website at {web-link} and on our website at {participating body's web-link}.

Level 2 – Condensed Text – to be published on Authority's website

As a public authority, 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.

The Auditor General is responsible for carrying out data matching exercises under its powers under the Public Audit (Wales) Act 2004.

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 fraudulent claims and payments to be identified. Where a match is found it indicates that there is 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 Auditor General currently requires us to participate in a data matching exercise to assist in the prevention and detection of fraud. The Auditor General requires this authority to provide information it holds for this purpose. We are required to provide particular sets of data to the Auditor General for matching. Details are set out on the Wales Audit Office website, www.wao.gov.uk.

As the use of data by the Auditor General in a data matching exercise is carried out with statutory authority (Part 3A of the Public Audit (Wales) Act 2004), it does not require the consent of the individuals concerned under the Data Protection Act 1998.

Data matching by the Auditor General is subject to a Code of Practice. This is to help all bodies involved in data matching to comply with the law and good practice, including maintaining data security (see www.wao.gov.uk).

For further information on the Auditor General's legal powers and the reasons why he matches particular information, see {web-link to Level 3 notice on Wales Audit Office website} or contact {name of Key Contact, email, address and phone number}.

Level 3 – Full Text – to be published on Wales Audit Office website

Auditor General's data matching exercises

The Auditor General conducts data matching exercises to assist in the prevention and detection of fraud.

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. Computerised data matching allows fraudulent claims and payments to be identified. Where a match is found it indicates that there is 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.

As the use of data by the Auditor General in a data matching exercise is carried out with statutory authority ((Part 3A of the Public Audit (Wales) Act 2004)), it does not require the consent of the individuals concerned under the Data Protection Act 1998.

All bodies participating in the Auditor General's data matching exercises receive a report identifying matching data within that body's own records and between that body's records and those of other relevant bodies. It is for the 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.

To date, the NFI has led to the detection of fraud and overpayments in Wales totalling some £7 million.

Legal basis

From 2008, the Auditor General will conduct data matching exercises under new statutory powers contained in the Public Audit (Wales) Act, as amended by the Serious Crime Act 2007. Previous exercises were undertaken under his value-for-money examination and study functions in the 2004 Act and the Government of Wales Act 1998, and under appointed auditor's powers.

Under the new powers:

- a** the Auditor General may carry out data matching exercises for the purpose of assisting in the prevention and detection of fraud;

- b** the Auditor General may require local government and NHS bodies in Wales to provide data for data matching exercises;
- c** other bodies and persons may participate in its data matching exercises on a voluntary basis where the Auditor General considers it appropriate. Where they do so, the statute states that there is no breach of confidentiality and generally removes other restrictions in providing the data to the Auditor General;
- d** the requirements of the Data Protection Act 1998 continue to apply;
- e** the Auditor General may disclose the results of data matching exercises where this assists in the prevention and detection of fraud, and for certain other purposes, to bodies that have provided the data and to the auditors that he appoints;
- f** the Auditor General may publish a summary report;
- g** the Auditor General may disclose both data provided for data matching and the results of data matching to the Audit Commission, the Comptroller and Auditor General for Northern Ireland, the Auditor General for Scotland, the Accounts Commission for Scotland and Audit Scotland, for the purposes of preventing and detecting fraud;
- h** wrongful disclosure of data obtained for the purposes of data matching by any person is a criminal offence;
- i** the Auditor General may charge a fee to any body participating in a data matching exercise;
- j** the Auditor General must prepare and publish a Code of Practice. All bodies conducting or participating in his data matching exercises must have regard to the Code, including the Auditor General himself.

Bodies required to provide or which volunteer data for matching

Currently, the Auditor General requires unitary local government authorities, police authorities, fire and rescue authorities, Local Health Boards (LHBs), NHS Trusts, probation boards and probation trusts to provide data. In addition, the following bodies provide data to the Auditor General for matching on a voluntary basis:

Welsh Assembly Government

[List of voluntary participating bodies to be updated from time to time]

The data that is matched and the reasons for matching it

For information describing which data sets are matched by the Auditor General and the purposes of each matching please refer to the Auditor General's guidance available on this website.

Code of Data Matching Practice

Data matching by the Auditor General is subject to a Code of Practice (see www.wao.gov.uk). This is to help all bodies involved in data matching to comply with the law and good practice, including maintaining data security.

Further information

More details on the Auditor General's data matching exercises, including national reports, other publications and guidance, may be found at www.wao.gov.uk. Further information on the NFI exercises may be found at <http://www.wao.gov.uk/whatwedo/1252.asp>.

Alternatively please contact the Wales Audit Office's NFI Co-ordinator, Wales Audit Office, 24 Cathedral Road, Cardiff, CF11 9LJ (nfi@wao.gov.uk).

Appendix 3 – Relevant statutory provisions

This appendix sets out extracts from the following statutory provisions:

- i** Schedules 1, 2 and 3 of the Data Protection Act 1998 – the data protection principles and fair processing requirements;
- ii** Section 27 of the Data Protection Act 1998 – exemptions;
- iii** Section 29 of the Data Protection Act 1998 – exemption in relation to crime and taxation;
- iv** Section 34 of the Data Protection Act 1998 – exemption in relation to information available by or under an enactment;
- v** Section 35 of the Data Protection Act 1998 – exemption in relation to disclosures required by law;
- vi** Section 31 of the Freedom of Information Act 2000 – exemption in relation to law enforcement;
- vii** Section 40 of the Freedom of Information Act 2000 – exemption in relation to personal information;
- viii** Section 64A of the Public Audit (Wales) Act 2004 – power to conduct data matching;
- ix** Section 64B of the Public Audit (Wales) Act 2004 – mandatory provision of data;
- x** Section 64C of the Public Audit (Wales) Act 2004 – voluntary provision of data; and
- xi** Section 64D of the Public Audit (Wales) Act 2004 – disclosure of results of data matching etc (including criminal offence).

i) The 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 for 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.

...

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,
 - (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
 - (iii) in any other case, the end of that period.

- (3) The information referred to in sub-paragraph (1) is as follows, namely—
- (a) the identity of the data controller,
 - (b) if he has nominated a representative for the purposes of this Act, the identity of that representative,
 - (c) the purpose or purposes for which the data are intended to be processed, and
 - (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.

3

- (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.
- (2) The primary conditions referred to in sub-paragraph (1) are—
- (a) that the provision of that information would involve a disproportionate effort, or
 - (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.

4

...

Schedule 2

Conditions Relevant for Purposes of the First Principle: Processing of any Personal Data

...

3

The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.

4

...

5

The processing is necessary—

- (a) for the administration of justice,
- (aa) ...
- (b) for the exercise of any functions conferred on any person by or under any enactment,
- (c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or
- (d) for the exercise of any other functions of a public nature exercised in the public interest by any person.

6

- (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.

- (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.

Schedule 3

Conditions Relevant for Purposes of the First Principle: Processing of Sensitive Personal Data

1

...

2

- (1) The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.

...

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,

...

- (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 sub-paragraph (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.

ii) Section 27 of the Data Protection Act 1998 – exemptions

Subject information and non-disclosure provisions

- (1) ...

- (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.

iii) Section 29 of the Data Protection Act 1998 – exemption in relation to 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) ...

(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.

...

iv) Section 34 of the Data Protection Act 1998 – exemption in relation to 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.

v) Section 35 of the Data Protection Act 1998 – exemption in relation to disclosures required by law

- (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) ...

vi) Section 31 of the Freedom of Information Act 2000 – exemption in relation to law enforcement

- (1) Information which is not exempt information by virtue of section 30 is exempt information if its disclosure under this Act would, or would be likely to, prejudice—
 - (a) the prevention or detection of crime;
 - (b) the apprehension or prosecution of offenders;

- ...
- (2) ...
- (3) The duty to confirm or deny does not arise if, or to the extent that, compliance with section 1(1)(a) would, or would be likely to, prejudice any of the matters mentioned in subsection (1).

vii) Section 40 of the Freedom of Information Act 2000 – exemption in relation to personal information

- (1) Any information to which a request for information relates is exempt information if it constitutes personal data of which the applicant is the data subject.
- (2) Any information to which a request for information relates is also exempt information if—
 - (a) it constitutes personal data which do not fall within subsection (1), and
 - (b) either the first or the second condition below is satisfied.
- (3) 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 by public authorities) were disregarded.

- (4) 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).
- (5) The duty to confirm or deny—
 - (a) does not arise in relation to information which is (or if it were held by the public authority would be) exempt information by virtue of subsection (1), and
 - (b) does not arise in relation to other information if or to the extent that either—
 - (i) the giving to a member of the public of the confirmation or denial that would have to be given to comply with section 1(1)(a) would (apart from this Act) contravene any of the data protection principles or section 10 of the Data Protection Act 1998 or would do so if the exemptions in section 33A(1) of that Act were disregarded, or
 - (ii) by virtue of any provision of Part V of the Data Protection Act 1998 the information is exempt from section 7(1)(a) of that Act (data subject's right to be informed whether personal data being processed).
- (6) ...

(7) 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’ has the same meaning as in section 1(1) of that Act;

‘personal data’ has the same meaning as in section 1(1) of that Act.

viii) Section 64A of the Public Audit (Wales) Act 2004 – power to conduct data matching exercises

- (1) The Auditor General for Wales may conduct data matching exercises or arrange for them to be conducted on his 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) is exercisable for the purpose of assisting in the prevention and detection of fraud in or with respect to Wales.
- (4) That assistance may, but need not, form part of an audit.
- (5) A data matching exercise may not be used to identify patterns and trends in an individual's characteristics or behaviour which suggest nothing more than his potential to commit fraud in the future.
- (6) In the following provisions of this Part, reference to a data matching exercise is to an exercise conducted or arranged to be conducted under this section.

ix) Section 64B of the Public Audit (Wales) Act 2004 – mandatory provision of data

- (1) The Auditor General for Wales may require—
 - (a) any body mentioned in subsection (2), and
 - (b) any officer or member of such a body, to provide the Auditor General or a person acting on his behalf with such data (and in such form) as the Auditor General or that person may reasonably require for the purpose of conducting data matching exercises.
- (2) The bodies are—
 - (a) a local government body in Wales (as defined in section 12(1));
 - (b) a Welsh NHS body (as defined in section 60).
- (3) A person who without reasonable excuse fails to comply with a requirement of the Auditor General under subsection (1)(b) 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.
- (4) If an officer or member of a body is convicted of an offence under subsection (3), any expenses incurred by the Auditor General in connection with proceedings for the offence, so far as not recovered from any other source, are recoverable from that body.

x) Section 64C of the Public Audit (Wales) Act 2004 – voluntary provision of data

- (1) If the Auditor General for Wales thinks it appropriate to conduct a data matching exercise using data held by or on behalf of a body or person not subject to section 64B, the data may be disclosed to the Auditor General or a person acting on his behalf.
- (2) A disclosure under subsection (1) does not breach—
 - (a) any obligation of confidence owed by a person making the disclosure, or
 - (b) any other restriction on the disclosure of information (however imposed).
- (3) But nothing in this section authorises a disclosure which—
 - (a) contravenes the Data Protection Act 1998 (c 29), or
 - (b) is prohibited by Part 1 of the Regulation of Investigatory Powers Act 2000 (c 23).
- (4) Data may not be disclosed under subsection (1) if the data comprise or include patient data.
- (5) ‘Patient data’ means data relating to an individual which are held for medical purposes (within the meaning of section 251 of the National Health Service Act 2006 (c 41)) and from which the individual can be identified.
- (6) This section does not limit the circumstances in which data may be disclosed apart from this section.
- (7) Data matching exercises may include data provided by a body or person outside England and Wales.

xi) Section 64D of the Public Audit (Wales) Act 2004 – disclosure of results of data matching etc

- (1) This section applies to the following information—
 - (a) information relating to a particular body or person obtained by or on behalf of the Auditor General for Wales for the purpose of conducting a data matching exercise,
 - (b) the results of any such exercise.
- (2) Information to which this section applies may be disclosed by or on behalf of the Auditor General for Wales if the disclosure is—
 - (a) for or in connection with a purpose for which the data matching exercise is conducted,
 - (b) to a body mentioned in subsection (3) (or a related party) for or in connection with a function of that body corresponding or similar to the functions of an auditor under Chapter 1 of Part 2 or the functions of the Auditor General under Part 3 or this Part, or
 - (c) in pursuance of a duty imposed by or under a statutory provision.
- (3) The bodies are—
 - (a) the Audit Commission,
 - (b) the Auditor General for Scotland,
 - (c) the Accounts Commission for Scotland,
 - (d) Audit Scotland,
 - (e) the Comptroller and Auditor General for Northern Ireland,

- (f) a person designated as a local government auditor under Article 4 of the Local Government (Northern Ireland) Order 2005 (S.I. 2005/1968 (N.I.18)).
 - (iv) a body to which Article 90 of the Health and Personal Social Services (Northern Ireland) Order 1972 (S.I.1972/1265 (N.I.14)) applies.
- (4) 'Related party', in relation to a body mentioned in subsection (3), means—
- (a) a body or person acting on its behalf,
 - (b) a body whose accounts are required to be audited by it or by a person appointed by it,
 - (c) a person appointed by it to audit those accounts.
- (5) If the data used for a data matching exercise include patient data—
- (a) subsection (2)(a) applies only so far as the purpose for which the disclosure is made relates to a relevant NHS body,
 - (b) subsection (2)(b) applies only so far as the function for or in connection with which the disclosure is made relates to such a body.
- (6) In subsection (5)—
- (a) 'patient data' has the same meaning as in section 64C,
 - (b) 'relevant NHS body' means—
 - (i) a Welsh NHS body as defined in section 60,
 - (ii) a health service body as defined in section 53(1) of the Audit Commission Act 1998 (c. 18),
 - (iii) an NHS body as defined in section 22(1) of the Community Care and Health (Scotland) Act 2002 (asp 5),
- (7) Information disclosed under subsection (2) may not be further disclosed except—
- (a) for or in connection with the purpose for which it was disclosed under paragraph (a) or the function for which it was disclosed under paragraph (b) of that subsection,
 - (b) for the investigation or prosecution of an offence (so far as the disclosure does not fall within paragraph (a)), or
 - (c) in pursuance of a duty imposed by or under a statutory provision.
- (8) Except as authorised by subsections (2) and (7), a person who discloses information to which this section applies is guilty of an offence and liable—
- (a) on conviction on indictment, to imprisonment for a term not exceeding two years, to a fine or to both, or
 - (b) on summary conviction, to imprisonment for a term not exceeding 12 months, to a fine not exceeding the statutory maximum or to both.
- (9) Section 54 does not apply to information to which this section applies.
- (10) In this section 'statutory provision' has the meaning given in section 59(8).

Appendix 4 – Contact details

General enquiries

For information on the Auditor General's data matching exercises please see <http://www.wao.gov.uk/whatwedo/1252.asp>.

Alternatively please contact the Wales Audit Office's NFI Co-ordinator, Wales Audit Office, 24 Cathedral Road, Cardiff, CF11 9LJ (nfi@wao.gov.uk).

Complaints

Complaints about bodies participating in the Auditor General's data matching exercises should be addressed to those bodies. Complaints about the Auditor General's role, or that of his staff or appointed auditors, in conducting data matching exercises will be dealt with under the Wales Audit Office complaints procedure. Such complaints can be made by phone, email or letter to the Complaints Manager, Wales Audit Office, 24 Cathedral Road, Cardiff CF11 9LJ, 029 2032 0500 or complaints@wao.gov.uk. Further details of the Wales Audit Office complaints procedure may be found at <http://www.wao.gov.uk/whoweare/howtocomplain.asp>.