Social Security Fraud Act 2001 (s.3(1))
Code of Practice on Obtaining Information
Version Two

April 2002

Contents

Disclaimer

This Code of Practice gives general guidance only and should not be regarded as a complete and authoritative statement of the law. If you do not understand any of the contents of the Code you may wish to seek independent advice.

Social Security Fraud Act 2001 (s.3(1))
Code of Practice on Obtaining Information
Version Two

Foreword

0.1 This is version two of the Code of Practice. Version one was issued and laid before Parliament on 28 January 2002.

0.2 The Code has been revised to take account of changes to the definitions of some information providers brought about by other legislation. Banks and insurers have been redefined in accordance with the provisions of the Financial Services and Markets Act 2000 and subsequent secondary legislation. We have also added distributors of gas and electricity, in addition to suppliers of these products, to take account of changes in the energy industry brought about by the Utilities Act 2000 and subsequent secondary legislation.

0.3 We have made an explicit reference to the Director of National Savings, to make it clear that Authorised Officers will have access to information about all National Savings products, not just those of the National Savings Bank.

0.4 Other minor changes have been to remove any references to the Benefits Agency, which ceased operations on 31 March 2002 and was succeeded by Jobcentre Plus, and to correct references to local authority Chief Finance Officers, erroneously referred to in version one as Principal Finance Officers.

0.5 We have also had the opportunity to revise paragraph 2.5, with the assistance of the Information Commissioner, to clarify the circumstances in which Authorised Officers can obtain information based on a description of a person.

0.6 This version will be issued on 30 April 2002, on commencement of the powers in Sections 1 and 2 of the Social Security Fraud Act 2001. It will be revised in one year's time.

Chapter one - Introduction

What is the purpose of this Code?

1.1 The Social Security Fraud Act 2001 (referred to as the Fraud Act) introduced powers for authorised Department for Work and Pensions (DWP) and local authority officers[1] to obtain information from listed organisations about their customers, in order to help combat fraud against the benefit system. Those powers were inserted into the Social Security Administration Act 1992 (referred to as the Administration Act) as amendments to existing provisions at Section 109B and 110A of that Act, and as new Sections 109BA and 110AA. This Code of Practice governs the use of these powers by officers of the DWP and local authorities. Authorised Officers must have regard to this Code when exercising the powers contained in the Fraud Act. Failure to observe the provisions of the Code of Practice does not of itself constitute an offence, but a court may have regard to the Code when considering if an officer has acted lawfully.

1.2 Examples of how the Fraud Act is likely to work are given throughout the Code. They are intended to be illustrative only. The examples should not be treated as a complete or authoritative statement of the law.

Who is this Code of Practice for?

1.3 This Code of Practice is intended for staff of the DWP who are authorised by the Secretary of State, under Section 109A of the Administration Act, to obtain information from persons set out in Section 109B(2A). It is also intended for local authority officers authorised by the Chief Executive or Chief Finance Officer under Section 110A of the Administration Act. The Code sets out how they should exercise the powers. This Code may also prove useful to persons from whom information may be required under these powers, and to members of the public who wish to know more about the powers.

Which organisations are required to provide information?

1.4 The organisations listed in the Fraud Act, for example banks, may hold information that could help to detect social security fraud. **A list of the organisations in question is given in Chapter Two.**

Who is authorised to request information?

1.5 Only officers that have received authorisation may make requests for information under these powers. They will have received full training in the correct application of

these powers. Authorised DWP Officers will work either in one of the Department's Operational Intelligence Units or the National Intelligence Unit. Local authorities may also authorise staff to use these powers for the purposes of investigating social security fraud. The numbers of Authorised Officers will be strictly limited. **More information about Authorised Officers is contained in Chapter Three.**

How should the powers be used?

1.6 In order to comply with provisions in the Human Rights Act 1998, these powers should be used as a last resort. Authorised Officers will be able to use them only where it is necessary to do so. This means that they must first consider whether the information is needed in order to uncover the facts. If the Authorised Officer decides that it is, they must then consider whether there are other less intrusive means of obtaining the information. This will include deciding whether the claimant should be approached in the first instance.

1.7 Authorised Officers will be able to request information in order to ensure that fraud can be detected and punished. For example, a building society may have information about a customer's savings account. If that customer is receiving a social security benefit on the grounds of having no savings or capital then he may be committing fraud. Knowing about that account may help DWP and local authorities to put a stop to the fraud. Under Section 111 of the Administration Act, any organisation that fails to provide information when asked to do so under these powers may be prosecuted. **More information on how the powers should be used can be found in Chapter Four.**

What are the safeguards against misuse of the powers?

1.8 Authorised Officers may obtain information only where they are allowed to by law, and they are obliged to maintain the security and confidentiality of all information that they may receive as a result of their duties. There are strict penalties for unauthorised requests for, or disclosure of, information. Comments or complaints about the use of these powers may be made to the manager of the Intelligence Unit in the case of DWP, or the local authority (or its contractor's) Fraud Manager, from whom the request has been made. Complaints about a local authority contractor's use of these powers may also be raised with the local authority itself. **More information about the safeguards against misuse of these powers and complaints is contained in Chapter Five.**

---

[1] Here and elsewhere in the Code the term 'local authority officers' includes those

working for companies sub-contracted to local authorities.

Chapter two - What are the powers?

Who can be required to provide information?

2.1 The Administration Act lists the organisations from which information may be required at Section 109B(2A). These are:

a. *any bank*[2], [4]

This includes: banks, credit unions, friendly societies, industrial and provident societies

aa. *the Director of National Savings*

b. *any person carrying on a business the whole or a significant part of which consists in the provision of credit (whether secured or unsecured) to members of the public*

For example, credit card companies and building societies

c. *any insurer*[3], [4]
d. *any credit reference agency (within the meaning given by Section 145(8) of the Consumer Credit Act 1974(c.39))*
e. *any body the principal activity of which is to facilitate the exchange of information for the purpose of preventing or detecting fraud*

For example, CIFAS the UK fraud avoidance system

f. *any person carrying on a business the whole or a significant part of which consists in the provision to members of the public of a service for transferring money from place to place*

For example, money transmission companies

g. *any water undertaker or sewerage undertaker, any water and sewerage authority constituted under Section 62 of the Local Government etc. (Scotland) Act 1994(c.39) or any authority which is a collecting authority for the purposes of Section 79 of that Act*
h. *any person who -*

(i) is the holder of a licence under Section 7 of the Gas Act 1986 (c.44) to convey gas through pipes, or

(ii) is the holder of a licence under Section 7A(1) of that Act to supply gas through pipes

i. *any person who (within the meaning of the Electricity Act 1989(c.29)) distributes or supplies electricity*
j. *any person who provides a telecommunications service*
k. *any person conducting any educational establishment or institution*
l. *any body the principal activity of which is to provide services in connection with admissions to educational establishments or institutions*
m. *the Student Loans Company*
n. *any servant or agent of any person mentioned in any of the preceding paragraphs.*

2.2 Any organisation covered by the description in the above list may be required to provide information to Authorised Officers. Authorised Officers are described in Chapter Three.

What types of information will be requested?

2.3 Authorised Officers will obtain any relevant information that is necessary to the prevention and detection of benefit fraud. For example, they may request such information as:

a. bank statements;
b. building society statements;
c. details of income from an insurance policy;
d. address records from a credit reference agency;
e. customer details from a utility company;
f. student status from the Student Loan Company.

2.4 Initial requests for information will not typically require detailed responses. For example, an Authorised Officer may ask a building society to provide a copy of the last quarter's statement in relation to a savings account. However, if this initial enquiry indicates that the fraud is of a more serious nature, for example, there are regular and substantial deposits made to the account, the Authorised Officer may request further, more detailed, information.

When and about whom may Authorised Officers require information?

2.5 Authorised Officers may only obtain information that relates to a particular person identified by name or description. In a minority of cases this may involve seeking to identify a suspected fraudster using his description (for example male, aged mid- thirties) and checking this against the address he uses. For example, in the case of a suspected fraudster involved in the bulk theft of benefit order books, we may contact a credit reference agency to find out if there is any one particular person matching the suspect's description (for example male, aged mid-thirties) listed at the address. If there is more than one possible match at that address we cannot require the agency to provide us with any information at all. We will do all we possibly can to eliminate any risk of our obtaining information about innocent third parties, which would be a breach of the Data Protection Act. Authorised Officers would not be able to ask the company to provide details of all customers living in a block of flats. Enquiries must be reasonable in relation to the purposes set out in the legislation.

2.6 The purposes to which DWP Authorised Officers must have regard are those set out at Section 109A(2) of the Administration Act. These are:

a. *ascertaining in relation to any case whether a benefit is or was payable in that case in accordance with any provision of the relevant social security legislation;*
b. *investigating the circumstances in which any accident, injury or disease which has given rise, or may give rise, to a claim for:*

    (i) industrial injuries benefit, or

    (ii) any benefit under any provision of the relevant social security legislation, occurred or may have occurred, or was or may have been received or contracted;

c. *ascertaining whether provisions of the relevant social security legislation are being, have been or are likely to be contravened (whether by particular persons or more generally);*
d. *preventing, detecting and securing evidence of the commission (whether by particular persons or more generally) of benefit offences.*

2.7 The purposes to which local authority Authorised Officers must have regard are those set out at Section 110A(2) of the Administration Act. These are:

a. *ascertaining in relation to any case whether Housing Benefit or Council Tax Benefit is or was payable in that case;*

b. *ascertaining whether provisions of the relevant social security legislation that relate to Housing Benefit or Council Tax Benefit are being, have been or are likely to be contravened (whether by particular persons or more generally); and*
c. *preventing, detecting and securing evidence of the commission (whether by particular persons or more generally) of benefit offences relating to Housing Benefit or Council Tax Benefit.*

2.8 Information providers will only be required to provide information that they keep as part of their normal business and will only be asked for information that they can reasonably be expected to hold. Authorised Officers cannot insist on information once they are informed that it is not kept. Authorised Officers must not ask for more recent information than that which is currently held. For example, they may not ask a utility company to obtain a current meter reading purely for the purposes of the fraud investigation. Information providers are not obliged to inform the Authorised Officer of enquiries that have been made by other law enforcement agencies.

2.9 The law also provides that an Authorised Officer may not make enquiries about an individual unless it appears to the Authorised Officer that there are reasonable grounds for believing that they are a person who has committed, is committing, or is intending to commit a benefit offence, or unless the individual is a family member of such a person.

2.10 This means that Authorised Officers may make enquiries where they have reasonable grounds for believing that a person is committing fraud, helping someone else to do so, or being lied about as part of a benefit claim in respect of them.

For example:

An anonymous tip-off is received alleging that a claimant is studying at a university without declaring the fact. If it is believed that the information is genuine and credible, an Authorised Officer may contact the university to confirm whether the claimant is currently a student. However, the Authorised Officer can make such an enquiry, in this example, only because he has received a credible allegation and therefore has reasonable grounds for suspicion.

2.11 Information may also be requested, for example, where it was suspected that a claimant had not disclosed capital held in a bank account. However, no information will be requested that is the subject of legal privilege - this is confidential communications between a legal adviser and his/her client for the purposes of giving or receiving legal

advice, or any information obtained or documentation prepared for the purposes of legal proceedings. For example, Authorised Officers may not request confidential client information from a bank's solicitor. However, information such as financial details contained in a loan application that does not constitute confidential communication for the purposes of obtaining legal advice and information concerned with the furthering of a criminal offence, is not protected by legal privilege.

2.12 Authorised Officers will only be able to make enquiries about family members where their circumstances are directly relevant to the claim being investigated. For example, if a man is claiming a means-tested benefit but not declaring his wife's earnings, Authorised Officers may make enquiries of her bank account in order to establish the truth.

2.13 A family is defined in Part 7, Section 137 of the Social Security Contributions and Benefits Act 1992 and associated regulations. A family is:

a. any married or unmarried couple who are members of the same household;
b. any married or unmarried couple who are members of the same household and any children or dependants which either member is responsible for and which live in the same household; and
c. a single person and any child or dependant which the person is responsible for and who lives in the same household.

2.14 Authorised Officers will not be able to make enquiries about family members who fall outside the definition given above. So, in the example, the Authorised Officer will not be able to make enquiries about a daughter who has left home and is working. However, if a member of the family is helping with the fraud - for example, a sister helping a relative to cash stolen order books - she could be guilty of a benefit offence, and could, therefore, be enquired about in her own right.

Who will we go to first for information?

2.15 Fraud investigators should always consider whether they could obtain the information they need from the claimant instead of asking an Authorised Officer to seek it from a third party. However, they will need to balance the risk of intrusion into the private life of the claimant with the risk that a determined fraudster may seek to further hide the truth when confronted by the investigator without corroborative evidence. When asking Authorised Officers to make a request for information they will include full documentation of the steps that have been made to seek the information by less intrusive means. If none have been taken full reasons will be provided.

[2] "bank" means - (a) a person who has permission under Part IV of the Financial Services and Markets Act 2000 (c.8) to accept deposits; (b) an EEA firm of the kind mentioned in paragraph 5(b) of Schedule 3 to that Act which has permission under paragraph 15 of that Schedule (as a result of qualifying for authorisation under paragraph 12 of that Schedule) to accept deposits or other repayable funds from the public; or (c) a person who does not require permission under that Act to accept deposits, in the course of his business in the United Kingdom.

[3] "insurer" means - (a) a person who has permission under Part IV of the Financial Services and Markets Act 2000 (c.8) to effect or carry out contracts of insurance; or (b) an EEA firm of the kind mentioned in paragraph 5(d) of Schedule 3 to that Act, which has permission under paragraph 15 of that schedule (as a result of qualifying for authorisation under paragraph 12 of that Schedule) to effect or carry out contracts of insurance.

[4] The definitions of "bank" and "insurer" must be read with (a) Section 22 of the Financial Services and Markets Act 2000; (b) any relevant order under that Section; and (c) Schedule 2 to that Act.

Chapter three - Who is authorised to use these powers?

The Authorised Officer

3.1 Only those DWP officers that have the Secretary of State's authorisation, or local authority officers that have been authorised by the Chief Executive or Chief Finance Officer may use these powers. These officers are known as Authorised Officers.

3.2 DWP will ensure that all enquiries are made through Authorised Officers working for one of the Operational Intelligence Units, or through the National Intelligence Unit. Their responsibility will be to make enquiries on behalf of fraud investigators. The numbers of staff eligible for authorisation will be limited to those who have received appropriate training (see paragraph 3.7).

3.3 Authorised Officers will hold a certificate of their authority and will be required to include a copy with enquiries whether they are made in writing, by fax or e-mail. Information providers will have access to a list of currently Authorised Officers (see "paragraph 4.23).

3.4 Authorised Officers have no direct role in making decisions on entitlement to benefit.

How will officers be authorised?

3.5 In DWP, the Fraud Area Manager acting on behalf of the Secretary of State will authorise officers. The Fraud Area Manager is an officer of Senior Executive Officer grade. Authorised Officers will be of management grades not below that of Executive Officer. They will be managed by officers not below the grade of Higher Executive Officer.

3.6 Local authority staff authorised to use these powers will be of a similar grade. They will be authorised by the officer designated under Section 4 of the Local Government and Housing Act 1989 as the head of the authority's paid service or the officer who is the authority's Chief Finance Officer (within the meaning of Section 5 of that Act).

How will officers be trained?

3.7 Authorised Officers, including those working for local authorities, must have received full training in the use of these powers. They must have completed appropriate training in investigative techniques, data protection and human rights legislation. This is contained

in relevant parts of the Professionalism in Security (PINS) syllabus or its equivalent. Authorised Officers will not be able to access on-line information until they have received suitable training.

Chapter four - How should the powers be used?

What will information providers need to know?

4.1 Information providers will need to know that they are legally obliged to provide information that has been properly requested in writing by an Authorised Officer. This obligation overrides any duty of customer confidentiality. This means that they cannot be held liable by their customers for providing information when the request is made in accordance with the law.

4.2 The Data Protection Act 1998 will not be contravened by providing the information requested by Authorised Officers. Under Section 35(1) of the Data Protection Act 1998 exemption from the non-disclosure provisions exists where a statutory provision, such as Section 109B and C of the Administration Act, requires the supply of information.

What details should requests for information contain?

4.3 All requests for information will include the following details.

a. the identity of the Authorised Officer who is making the request, and to whom the information should be sent;
b. sufficient information to ensure that the customer, and the particular account in question, can be identified from the information provided (see paragraph 4.25). This may include such detail as a date of birth, address or customer reference number; and
c. the address to which the information must be sent.

To whom should enquiries be addressed?

4.4 All enquiries will be made to the organisation involved. This is because it is organisations that are listed in the legislation (Section 109A(2A) of the Administration Act) on whom the requirement to provide information is placed. The DWP Professional Standards Unit will maintain a list of information providers who have specified a central point of contact for requests. This list will be made available to Authorised Officers. If an organisation nominates a particular person then enquiries will be to the organisation care of that person. If an individual has not been nominated, then the enquiry must be addressed to the organisation, care of the most senior individual within that organisation that the Authorised Officer can identify. If there were evidence of intentional failure to provide information it would be the organisation that faced prosecution and not the individual. Initially, refusals would be taken to the most senior level in an organisation in

order to secure compliance with a request. In exceptional circumstances, it is possible that only an individual rather than the precise name of an organisation could be identified. Where this happened then the request would be made to the most senior person that could be identified and they would be personally liable for not meeting the request.

4.5 DWP will enter into agreements with organisations as to where enquiries should be addressed and will inform local authorities of those arrangements. Where such arrangements exist the DWP and local authorities must abide by them.

What happens when an organisation fails to provide information?

4.6 If information is not provided the Authorised Officer should explain the statutory nature of the powers, and the potential consequences of non-compliance. Information providers will be expected to comply with requests and the matter will be taken further if an individual employee or corporate body is being obstructive. If a reasonable excuse for not providing the information has been given, the Authorised Officer must not insist on obtaining the information. Examples may include industrial action or a computer breakdown. This list is not exhaustive.

4.7 Information providers will be expected to comply with requests within a reasonable time scale. This will usually be within ten working days although, in exceptional cases, information may be required more urgently. If an information provider is unable to comply within ten working days, they should inform the Authorised Officer of the reason. If they are able to provide some but not all of the information within ten working days, they should do so and inform the Authorised Officer of the date that the full information is likely to be provided.

4.8 No one is required to provide any information that tends to incriminate themself or their spouse. No one may be required to provide information subject to legal professional privilege (see "paragraph 2.11). Otherwise there is a statutory duty to provide that information. Under Section 111 of the Administration Act, it is an offence to refuse, or neglect, to provide information that has been lawfully requested under these powers. Failure to meet in full requests for information could result in criminal proceedings being instigated. The maximum penalty is a fine, fixed at level 3, currently set at £1, 000, with a continuing penalty of £40 per day (under Section 111(2) of the Administration Act).

What are reasonable grounds?

4.9 Under no circumstances will Authorised Officers use these powers unless they think

it is reasonable to do so. What is reasonable will vary, depending on the circumstances of the case, and each case should be considered on its own merits. The decision of the Authorised Officer will be judged against what another person acting in good faith and in the same situation as the Authorised Officer might consider to be reasonable. Examples of what an Authorised Officer would consider when deciding whether or not his/her use of these powers is reasonable include:

a. whether there is a question that needs an answer;
b. whether he/she actually needs the information;
c. whether there was a less intrusive way of obtaining the information; and
d. whether the information could be obtained from the customer without jeopardising the investigation.

4.10 Authorised Officers will consider all the facts of the case known to them at that time when deciding what is reasonable. They will ensure that each decision made relating to the use of the powers will be documented and be available for checking by management or validators.

For example:

An Authorised Officer has received evidence suggesting that a claimant may be part of a gang defrauding the social security system. Were a fraud investigator to question the claimant immediately, he would risk tipping off the other members of the gang and give them time to conceal or destroy evidence. In these circumstances, it is unlikely that the investigator would contact the claimant before an Authorised Officer has gathered further information.

A claimant has declared savings of £2, 000 on his initial claim form. Some time later, an allegation is received that his savings are more substantial than this. In this instance, the investigator should question the claimant in the first instance, and he may be asked to provide copies of his bank or building society statements. If he refused, the investigator should ask for permission to contact his bank or building society directly. If he still refused, the investigator should ask an Authorised Officer to make an enquiry of the bank or building society under the terms of the Fraud Act.

An investigator has obtained a statement from an employer which appears to confirm that a claimant is in full-time employment. The investigator asks an Authorised Officer to obtain detailed bank statements to confirm the employer's statement and possibly uncover other undisclosed income. There is no reason to suppose that the employer's statement is inaccurate. Neither does the investigator explain why he has reasonable

grounds to suspect that there is any other undisclosed income. The Authorised Officer consequently rejects the request as the information is neither necessary nor are there reasonable grounds to suspect the existence of undisclosed income.

4.11 Management checks will ensure that these procedures are followed correctly. Any enquiry made without good reason could lead to disciplinary action against the officer concerned (see "paragraph 5.6).

How will information be requested?

4.12 All requests for information will be made in writing (by post, fax or e-mail) with regard to preferences expressed by information providers.

4.13 Authorised Officers will not make enquiries in person by means of a visit. However, they may make arrangements to telephone the organisation if they need to discuss the information that has been provided. No new enquiries will be made in the course of this contact.

4.14 Authorised Officers will not issue requests by either fax or e-mail without prior agreement with the information provider. Information providers will be able to make replies in a way that has been agreed with the Authorised Officer. Authorised Officers must take account of what would suit the organisation providing the information when deciding how information should be returned - for example, if the Authorised Officer makes a request by e-mail, it would not oblige the information provider to reply in the same manner. Where DWP or a local authority has entered into an agreement with an organisation as to how enquiries will be made and how information should be provided, Authorised Officers will comply with those arrangements when making requests.

4.15 Authorised Officers will make enquiries of specific information providers only where they have reasonable grounds for believing that they hold information on a particular individual. For example, Authorised Officers will not normally issue requests to all UK banks asking if they have information on a particular customer. However, such requests may be made in a small number of the most serious cases where the information cannot be obtained by other means. This would only be done in consultation with the intelligence unit or local authority fraud manager.

How will electronic access be managed?

4.16 DWP and local authorities may enter into arrangements to obtain information

electronically where an organisation is already prepared to provide such access to DWP or another organisation. The Secretary of State and local authorities may not require an organisation to enter into arrangements to provide electronic access if they are not already providing such access, or are not prepared to provide it, to another organisation - for example, they may not require such access because an organisation provides electronic access to records for its own employees, or because it provides a service whereby customers can electronically access their own accounts. The Secretary of State and local authorities will not require organisations to update their computer software in order to provide electronic access.

4.17 Local authorities may enter into agreements to provide electronic access to information only with the consent of the Secretary of State. Local authorities who do not have this consent may ask the DWP to make electronic enquiries on their behalf, or may approach the organisation concerned in writing. Local authorities must comply with any directions issued by the Secretary of State regarding payment for information.

4.18 The Secretary of State will provide local authorities with information on what they must do in order to obtain his consent to enter into arrangements for electronic access. He will need to be assured that a local authority has sufficient controls in place to enable on-line access to be properly monitored and to guard against misuse.

4.19 Local authorities need to obtain the Secretary of State's consent to the general use of the powers to obtain information electronically as set out in Section 109B of the Administration Act. Once they have obtained his general consent, they do not need further consent each time they wish to use the power. They must, however, comply with any directions issued in relation to arrangements such as those relating to payment for information. Nor do they need consent to enter into arrangements for electronic access to information already available - such as electronic access to an electoral roll.

4.20 When Authorised Officers access information electronically, they will ask only for information that they might otherwise have asked for manually. All requests must be necessary and reasonable.

4.21 Access to electronic information will be allowed only to specifically Authorised Officers. Such access will be controlled by passwords or equivalent. DWP and local authorities will also obtain a record of all enquiries in order that this can be cross-checked against their own records.

How will Authorised Officers manage requests for information?

4.22 DWP will ensure that all enquiries are made through centralised Intelligence Units. These units will process enquiries from DWP fraud investigators. Local authorities must take all reasonable steps to keep to a minimum the number of officers authorised to use these powers and to centralise enquiries within the local authority. Local authorities should consider whether it would be possible to work with another local authority in order to reduce the number of sources from which organisations may receive requests for information.

4.23 DWP and local authorities will make sure that adequate provisions are in place to guarantee the security of the arrangements for managing requests for information. Information providers will have access to a secure and up-to-date list of current Authorised Officers. This will be maintained by the DWP Professional Standards Unit who will ensure that only currently Authorised Officers who have received full training are included on the list. If a request is received from an officer who does not appear on the list, it should be refused and the information provider should contact the Intelligence Unit, or local authority, for further guidance. When requests are made, information providers will be told:

a. the name of the Authorised Officer making the request;
b. the address of the Intelligence Unit or local authority to which they belong; and
c. the name of the intelligence unit manager or local authority Fraud Manager.

Information providers can thereby be satisfied that requests are genuine and that they will need only deal with specified staff.

4.24 DWP and local authorities will manage requests in such a way as to cause the least inconvenience to the data provider. If, for example, a bank has nominated a central point of contact within its organisation for receiving enquiries, DWP and local authorities will be expected to direct their enquiries to it. DWP will pass details of any such agreement to local authorities and they will abide by them also.

4.25 DWP and local authorities will negotiate with information providers to ensure that the burdens on business are kept to a minimum. There will be established security protocols, such as passwords, to safeguard the information that is requested. DWP and local authorities will also agree specifications as to what information is required, in what form the request is made and in what form it will be received. If an agreement has been reached with an organisation as to the format in which information should be provided, Authorised Officers must accept the information in that format unless there are good grounds why that format is not appropriate in a particular instance. If this is the case, Authorised Officers must reach a specific agreement with the information provider in that

instance, explaining why they need to depart from normal procedures. As far as possible, DWP will seek agreements that are acceptable to local authorities.

How will information be used?

4.26 Information received from organisations in the private and public sector will be treated in exactly the same way as information received from any other source. The information that is received will also be weighed in the same way as information received from any other source. In the event that a criminal offence comes to light, such information may be laid before a court in such a way as it considers appropriate.

4.27 If as a result of the proper exercise of these powers a discrepancy is discovered that may affect entitlement to benefit, and that discrepancy cannot be explained by official error, the claimant may be asked for an explanation. If the explanation is not satisfactory, or if no explanation is offered, the case will be referred to a Decision Maker for a decision as to whether or not benefit should continue to be paid. Rights of appeal against decisions are not affected in any way by the use of these powers.

Information sharing

4.28 Section 122 of the Administration Act and Section 110 of the Finance Act 1997 enable the DWP, the Inland Revenue and HM Customs and Excise to share information for the prevention and detection of fraud and to ensure the accuracy of the information held by each Department. If information is received which suggests that taxes are being evaded, or that another crime is being committed, then DWP will pass on relevant information to other departments and local authorities.

4.29 Local authorities may provide information to DWP and may exchange information with each other for the purposes of administering Housing Benefit and Council Tax Benefit.

4.30 Under these powers, information may not be obtained for purposes other than the prevention or detection of benefit fraud. Local authorities will not obtain information on behalf of government departments or agencies. They may make enquiries on behalf of other local authorities only if they have the explicit authorisation of that authority. DWP may obtain information on behalf of a local authority, but not on behalf of another department or agency.

4.31 The procedures and standards which are to be adhered to for the disclosure of information and for the prevention of unauthorised disclosure are already enshrined in

law and in existing guidance to staff. These provisions ensure that those who obtain or disclose information unlawfully can be punished, thereby providing a deterrent against misuse.

4.32 The DWP Protection of Customer Information Guide, or its local authority equivalent, must be adhered to by staff in respect of all information, including that obtained under these powers. These define all the circumstances in which disclosure can occur.

Who will receive payment?

4.33 The Secretary of State has the power to make payment to information providers in certain circumstances. These are:

a. credit reference agencies;
b. telecommunications companies;
c. utilities where we are obtaining bulk information; and
d. the servants and agents of the above.

4.34 The DWP and local authorities will enter into negotiation with information providers in these categories to decide when payment is appropriate and how much will be paid. However, local authorities must follow any directions given by the Secretary of State regarding payment for information.

Chapter five - Safeguards

Confidentiality and security

5.1 Authorised Officers who obtain information from organisations in the public and private sector are bound by law to observe confidentiality and security at all times. The DWP and local authorities have strict procedures that aim to ensure that:

a. information is only used for lawful purposes notified to the Information Commissioner (see paragraph 5.5);
b. access to personal information is limited to those staff who need it to carry out their work; and
c. personal information is only disclosed to someone else where it is necessary and lawful to do so.

5.2 Records are kept of all access to electronic information using the powers in the Fraud Act (electronic access is covered in more detail at "paragraph 4.16). This means that management knows who has accessed the information, on whose behalf and for what reason. Management will undertake regular checks.

5.3 Each DWP Area employs a team of specialists responsible for probity issues amongst intelligence, administrative and investigative staff. They are independent and entirely separate from the investigative process and provide an extra tier of assurance. Data Managers will have random access to all enquiries made. They will provide periodic reports to senior managers and will identify any failure to follow proper procedures. They will, for example, audit all test-checking procedures to ensure that all management checks are carried out thoroughly and regularly.

The fair collection of data

5.4 The first data protection principle requires that information obtained by the use of these powers be collected lawfully and fairly. The Fraud Act provides for the lawful processing of such information. DWP and local authority claim forms and leaflets will inform customers that information may be sought about them from certain third parties. DWP will also work with data providers to ensure that their customers are aware of the possibility of disclosure under the new powers.

The Information Commissioner

5.5 The Information Commissioner is responsible for the promotion of good practice regarding the processing of personal data. She may take action for a breach of the Data Protection Act 1998. Further information can be obtained from:

The Office of the Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

Penalties for unlawful disclosure

5.6 If it appears that Authorised Officers have obtained or disclosed information unlawfully, or attempted to do so, they will be investigated. DWP and local authority disciplinary procedures can lead to dismissal and prosecution. Criminal offences include:

a. the unauthorised disclosure of social security information (Section 123 of the Administration Act). An offence under this Act is punishable by imprisonment for up to two years and/or a fine;
b. unauthorised access to computers (Section 1 of the Computer Misuse Act 1990). An offence under this Act is punishable by imprisonment for up to six months and/or a fine; and
c. the unlawful obtaining or disclosure of personal data (Section 55 of the Data Protection Act 1998).

Retention and storage

5.7 Under provisions in the Data Protection Act 1998, information may not be stored if it is not needed. DWP and local authority staff should follow the guidance provided to them by their organisation.

5.8 In DWP, information will be retained in accordance with the Department's guidance on retention of information. That is, it will usually be kept for not more than 18 months before being destroyed, unless it is required to be retained under the provisions of the Criminal Procedures and Investigation Act 1996, the Regulation of Investigatory Powers Act 2000 or for continuing debt recovery.

5.9 When information is obtained, it will be kept in secure storage conditions and may be accessed only by the Authorised Officer or Fraud Investigator to whom the information has been referred.

Complaints

5.10 A senior DWP official oversees professional standards for DWP and local authority investigators. He is the Chief Investigation Officer and Head of Profession for Fraud Investigators.

5.11 If anyone has a question about the way that an Authorised Officer has used their powers, or the reasonableness of their actions when obtaining information, they can contact the Authorised Officer to discuss the matter. For example, if compliance with a request for information can be made only at disproportionate cost, the information provider may inform the Authorised Officer of the fact and ask for the request to be reconsidered.

5.12 If this does not provide a satisfactory resolution to the matter they may write to the manager at the DWP Operational Intelligence Unit. Most complaints can be settled by contact with the local manager in this way, and it is the most effective way of putting things right. However, if the complaint is more serious, it should be directed to the DWP Fraud Area Manager.

5.13 Local authorities are independent statutory bodies with responsibility for the administration of Housing Benefit and Council Tax Benefit. Each authority has its own mechanism for handling complaints about the way in which it operates. If the complaint relates to the way that a local authority Authorised Officer has used the powers, reference should be made to the complaints procedure that each local authority has in place.

5.14 If this does not provide a satisfactory outcome, the complaint will be passed to the Professional Standards Unit for counter-fraud investigations, who will send a reply as soon as possible. An acknowledgement of receipt of the complaint will be sent within 10 working days. The Professional Standards Unit may seek legal advice before replying in full. Their address is as follows:

Professional Standards Unit
5th Floor West
Trevelyan Square
Boar Lane
Leeds LS1 6EB

5.15 Serious complaints relating to local authority use of electronic access should be

addressed to the Chief Executive of the local authority concerned. A copy of any enquiries or complaints should be sent to the Head of Profession at the Professional Standards Unit. Any complainant in these circumstances should contact both the local authority concerned and the DWP.

The Parliamentary Ombudsman

5.16 The Parliamentary Commissioner for Administration (or Parliamentary Ombudsman as he is commonly known) deals with complaints about maladministration by public bodies. Any complaint must be made via a Member of Parliament. The Ombudsman seeks to establish whether a public body has acted correctly and fairly in carrying out its interpretation of the law. Cases for investigation may include those where a public authority is alleged to have done something in the wrong way, done something they should not have done or failed to do something which they should have done. The Ombudsman can recommend a variety of remedies, including the payment of compensation to complainants and the revision, adherence to, or clarification, of administrative procedures. Further information can be obtained from:

The Office of the Parliamentary Commissioner for Administration
Millbank Towers
Millbank
London SW1P 4QP

The Local Government Ombudsmen

5.17 The Local Government Ombudsmen investigate complaints of injustice arising from maladministration by local authorities and certain other bodies. There are three Local Government Ombudsmen in England and one each for Scotland and Wales. They each deal with complaints from different parts of the country and investigate complaints about most council matters. Further information can be obtained from:

England
Local Government Ombudsman
21 Queen Anne's Gate
London SW1H 9BU

Scotland
Local Government Ombudsman
23 Walker Street
Edinburgh EH3 7HX

Wales
Local Government Ombudsman
Derwen House
Court Road
Bridgend CF31 1BN

Subject Access

5.18 The Data Protection Act 1998 gives individuals the right of 'subject access' and the leaflet GL33 *The Data Protection Act 1998: It affects you* tells DWP customers how the Data Protection Act affects them. The right of subject access means that, with certain exceptions, a person has the right to request, and be given, information by data controllers. Exceptions include where the release of information following such a request would be likely to prejudice the prevention or detection of crime or the apprehension or prosecution of offenders. Under Part 2, Section 7 of the Act, an individual is entitled to be informed, upon request, by a data controller:

a. whether he or she is the subject of any data being processed by the controller;
b. if so, to be given a description of the personal data, the purposes for which the data are being processed and information about anyone else the data may have been disclosed to; and
c. to be given a copy of the personal data held about them and be told where the data were obtained from, and where the individual has been subject to an automated decision, to be told about the logic involved in that decision.

5.19 A data controller must provide the information promptly and at least within 40 days of receiving the request.

5.20 Anyone wishing to be provided with this information about data on DWP computer systems or any personal information held about them by the DWP should write to their local social security office.

5.21 Anyone wishing to be provided with information about data on local authority computer systems or any personal information held about them should write to their local authority.

Appeals against benefit decisions

5.22 Customers' normal rights of appeal are not affected by the use of powers to obtain

information from the private and public sector. A customer has the right to dispute or appeal against a benefit decision, including a decision based on the results of an investigation into an inconsistency identified by the use of these powers. If the customer has disputed the decision but remains dissatisfied with the outcome, they can still appeal in the usual way.

5.23 The leaflet GL24 *If you think our decision is wrong* tells customers how to dispute and appeal a decision made by the Secretary of State; further details can be found in leaflet NI260DMA *A guide to dispute, supersession and appeal*. These leaflets are available from social security offices or on the DWP website. Local authorities will have similar provisions.

5.24 If a customer is not satisfied with the way in which their case is managed, they should contact the relevant DWP or local authority office. The complaint will be dealt with as quickly as possible. The leaflet GL22 *Tell us about your comments and complaints* is available from social security offices and post offices. This leaflet also explains the circumstances in which compensation will be considered. Local authorities will have similar arrangements.