

Covering letter for internet

Social Security Fraud Act (Northern Ireland) 2001 Code of Practice on Obtaining Information Version Two

February 2003

Contents

Foreword

Chapter One

Chapter Two

Chapter Three

Chapter Four

Chapter Five

Introduction

What are the powers?

Who is authorised to use the powers?

How should the powers be used?

Safeguards

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.

DEPARTMENT for SOCIAL DEVELOPMENT

**SOCIAL SECURITY FRAUD ACT
(NORTHERN IRELAND)
2001**

**CODE OF PRACTICE
ON OBTAINING INFORMATION**

VERSION TWO

This Code of Practice is also available to members of the public through SSA offices and on the Department's website (www.dsdni.gov.uk).

CONTENTS

FOREWORD	3
CHAPTER ONE	
Introduction	4
CHAPTER TWO	
What Are The Powers?	7
CHAPTER THREE	
Who Is Authorised To Use The Powers?	12
CHAPTER FOUR	
How Should The Powers Be Used?	13
CHAPTER FIVE	
Safeguards	20

FOREWORD

- 0.1 This is version two of the Code of Practice. Version one was issued and laid before the Assembly on 19 December 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, so that information can be obtained to identify the supplier to a particular household.
- 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 This version will be issued on 24 February 2003, on commencement of the powers in sections 1 and 2 of the Social Security Fraud Act (Northern Ireland) 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 (Northern Ireland) 2001 (referred to as the Fraud Act) introduced powers for Authorised Officers from the Department for Social Development and authorities administering Housing Benefit¹ 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 (Northern Ireland) Act 1992 (referred to as the Administration Act) as amendments to existing provisions at section 103B and 104A of that Act, and as new sections 103BA and 104AA. This Code of Practice governs the use of these powers by Officers of the Department. 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 who are authorised by the Department, under section 103A of the Administration Act, to obtain information from persons set out in section 103B(2A) of that 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. **Although the authorities administering Housing Benefit have the right to exercise these powers, it is not their intention to use them at present. This does not however prevent them from doing so in the future. This Code of Practice only makes reference to authorised officers from the Department.**

¹ Here and elsewhere in the Code the term “authorities administering Housing Benefit” means the Northern Ireland Housing Executive and the Rate Collection Agency (which is an executive agency of the Department of Finance and Personnel).

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 who have received authorisation by the Department may make requests for information under these powers. They will have received full training in the correct application of these powers. The Authorised Officers will work in the Department's Operational Intelligence Unit. 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 the Authorised Officer must have first considered 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 less intrusive means of obtaining the information. This will include deciding whether the customer should be approached in the first instance.
- 1.7 Authorised Officers will be able to request information when it is necessary 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 they may be committing fraud. Knowing about that account may help the Department to put a stop to the fraud. Under section 105 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 at 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 Benefit Investigation Services. **More information about the safeguards against misuse of these powers and complaints is contained in Chapter Five.**

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 103B(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)*⁵

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 credit industry fraud avoidance system

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 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.

5 C.39

- 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 person who is the holder of a licence under Article 8(1) of the Gas (Northern Ireland) Order 1996(a) which relates to the conveyance or supply of gas through pipes*
- h. Any person who is the holder of a licence under Article 10(1) of the Electricity (Northern Ireland) Order 1992(a) which relates to the transmission or supply of electricity*
- i. Any person who provides a telecommunications service*
- j. Any person conducting any educational establishment or institution*
- k. Any body the principal activity of which is to provide services in connection with admissions to educational establishments or institutions*
- l. The Student Loans Company (any body to whom functions are delegated by arrangements made under Article 4(3) of the Education (Student Support) (Northern Ireland) Order 1998)*
- m. 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 for 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; and
 - f. student status from the Student Loans 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 there may be fraud 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 that is relevant to the investigation.

When and about whom may Authorised Officers require information?

- 2.5 Authorised Officers may only obtain information that relates to a particular individual identified by name or description. In a minority of cases this may involve seeking to identify a suspected fraudster using his description (eg 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 individual matching the suspect's description listed at that 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 1998. 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 Authorised Officers from the Department must have regard are those set out at section 103A(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); and*
 - d. *preventing, detecting and securing evidence of the commission (whether by particular persons or more generally) of benefit offences.*
- 2.7 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.
- 2.8 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.

- 2.9 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 misrepresented as part of a benefit claim in respect of them.

For example:

An anonymous tip-off is received alleging that a customer 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 customer 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.

- 2.10 Information may also be requested, for example, where it was suspected that a customer 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 communication between a legal advisor 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.
- 2.11 Authorised Officers will only be able to request from any person providing a telecommunications service, information which (within the meaning of section 21 of the Regulation of Investigatory Powers Act 2000) is communications data but not traffic data.
- 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 section 133 of the Social Security Contributions and Benefits (Northern Ireland) 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 Authorised Officers go to first for information?

2.15 Fraud investigators should always consider whether they could obtain the information they need from the customer 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 customer 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.

CHAPTER THREE

Who Is Authorised To Use These Powers?

The Authorised Officer

- 3.1 Only those officers that have the Department's authorisation, may use these powers. These officers are known as Authorised Officers.
- 3.2 The Department will ensure that all enquiries are made through Authorised Officers working in the Operational 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 3.6).
- 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 4.20).
- 3.4 Authorised Officers have no direct role in making decisions on entitlement to benefit.

How will officers be authorised?

- 3.5 The Manager of Benefit Investigation Services acting on behalf of the Department will authorise officers. The Manager is an officer of Deputy Principal 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 Staff Officer.

How will officers be trained?

- 3.6 Authorised Officers 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 and be aware of their responsibilities under section 75 of the Northern Ireland Act 1998. This is contained in relevant parts of the Professionalism in Security 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 properly requested by Authorised Officers. Under section 35(1) of that Act exemption from the non-disclosure provisions exists where a statutory provision, such as sections 103B and 103C 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 in a secure manner;
 - b. sufficient information to ensure that the customer, and the particular account in question, can be identified from the information provided (see paragraph 4.20). This may include such detail as a date of birth, address or customer reference number;
 - c. the address of the Operational Intelligence Unit to which the information must be sent; and
 - d. the name of the Operational Intelligence Unit manager.

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 103B(2A) of the Administration Act) on whom the requirement to provide information is placed. The Fraud Policy 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 individual then enquiries will be to the organisation, care of that

individual. 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 individual that could be identified and they would be personally liable for not meeting the request.

- 4.5 The Department will enter into agreements with organisations as to where enquiries should be addressed. Where such arrangements exist, the Department 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 themselves or their spouse. No one may be required to provide information subject to legal privilege (see paragraph 2.10). Otherwise there is a statutory duty to provide that information. Under section 105 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 maximum fine, fixed at level 3, currently set at £1,000, with a continuing penalty of £40 per day (under section 105(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 must 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 should consider when deciding whether or not their use of these powers is reasonable include:

- a. whether there is a question that needs an answer;
- b. whether they actually need the information;
- c. whether there is 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 auditors.

Examples:

An Authorised Officer has received evidence suggesting that a customer may be part of a gang defrauding the social security system. Were a fraud investigator to question the customer 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 customer before an Authorised Officer has gathered further information.

A customer 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 case, the investigator should question the customer 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 consider making an enquiry of the bank or building society under the terms of the Fraud Act.

An investigator has obtained a statement from an employer that appears to confirm that a customer is in full time employment. The investigator asks an Authorised Officer to obtain detailed bank statements to confirm the employers 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 the Department 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 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 Operational Intelligence Unit manager.

How will electronic access be managed?

- 4.16 The Department may enter into arrangements to obtain information electronically where an organisation is already prepared to provide such access to the Department or another organisation. The Department 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 Department will not require organisations to update their computer software in order to provide electronic access.
- 4.17 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.
- 4.18 Access to electronic information will be allowed only to specifically Authorised Officers. Such access will be controlled by passwords or equivalent. The Department 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?

- 4.19 The Department will ensure that all enquiries are made through the Operational Intelligence Unit. This Unit will process enquiries from the Department's fraud investigators.
- 4.20 The Department 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 held by the Department's Operational Intelligence Unit. Only currently Authorised Officers who have received full training will be 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 Operational Intelligence Unit for further guidance. For details of what should be contained in requests to information providers, see paragraph 4.3.
- 4.21 The Department will manage requests in such a way as to cause least inconvenience to the information provider. If, for example, a bank has nominated a central point of contact within its organisation for receiving enquiries, the Department will be expected to direct their enquiries to it.
- 4.22 The Department 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 or equivalent, to safeguard the information that is requested. The Department 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.

How will information be used?

- 4.23 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.
- 4.24 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 customer 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

- 4.25 Section 116 of the Administration Act and section 110 of the Finance Act 1997 enable the Department, 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 fraud is occurring or that another crime is being committed, then the Department will pass on relevant information to the appropriate Department.
- 4.26 Authorities administering Housing Benefit may provide information to the Department and may exchange information with each other for the purposes of administering Housing Benefit.
- 4.27 Under these powers, information may not be obtained for purposes other than the prevention, investigation or detection of benefit fraud. The Department may obtain information on behalf of the authorities administering Housing Benefit, but not on behalf of another Department or agency.

- 4.28 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.
- 4.29 The Department's Protection of Customer Information Guide must be adhered to by staff in respect of all information, including that obtained under these powers. This guide defines all the circumstances in which disclosure can occur.

Who will receive payment?

- 4.30 The Department 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.
- 4.31 The Department will enter into negotiation with information providers in these categories to decide when payment is appropriate and how much will be paid.

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 Department has 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 The Department's Internal Audit is responsible for providing assurance on probity issues amongst intelligence, administrative and investigative staff within the Department. They are independent and entirely separate from the investigative process. They provide an extra tier of assurance and 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. The Department's claim forms and leaflets will inform customers that information may be sought about them from certain third parties. The Department will also work with information 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, and may prosecute anyone who breaches the Data Protection Act. 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. The Department's disciplinary procedures can lead to dismissal and prosecution. Criminal offences include:
- a. the unauthorised disclosure of social security information (section 117 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. The Department's staff should follow the guidance provided to them by their organisation.
- 5.8 In the Department, 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 14 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 The leaflet '*Making a Complaint*' is available from Social Security Offices and Advisory Groups. In all cases an acknowledgement of receipt of the complaint will be sent within 2 working days and normally a full response will be issued within 10 working days.
- 5.11 A senior Departmental official oversees Social Security Agency investigators. He is the Director of Benefit Security.
- 5.12 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.
- 5.13 If this does not provide a satisfactory resolution to the matter they may write to the Manager of Benefit Investigation Services. Most complaints can be settled by contact with the 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 Head of Benefit Security Services. Their addresses are as follows:-

Manager of Benefit Investigation Services
2 Curtis Street
BELFAST
BT1 2ND

Head of Benefit Security Services
2 Curtis Street
BELFAST
BT1 2ND

- 5.14 Anyone who remains dissatisfied may write to the Agency's Chief Executive and ask him to look into the complaint. The Chief Executive will ask the Customer Services Director to investigate and reply on his behalf. His address is as follows:-

Chief Executive
Social Security Agency
Churchill House
Victoria Square
BELFAST BT1 4SS

- 5.15 If, having received a reply from or on behalf of the Chief Executive, any member of the public is not satisfied they can have a complaint investigated by the Independent Case Examiner. The Independent Case Examiner will act as an independent referee if any customer feels that the Agency has treated them unfairly or they are not happy with the way we have dealt with their complaint. The address is as follows:

Independent Case Examiner
PO Box 1245
BELFAST
BT2 7DF

- 5.16 The Department welcomes feedback. Although we make every effort to get things right, occasionally we may get things wrong. We want to know how we can put things right and we want to learn from our mistakes.

The Ombudsman

- 5.17 The Ombudsman deals with complaints about maladministration by government departments and their agencies. Any complaint should be sponsored by a member of the Northern Ireland Assembly. The Ombudsman seeks to establish whether the public body has acted correctly in accordance with established policies and procedures. 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 an apology, a consolatory payment or the revision or clarification of administrative procedures.

Further information can be obtained from:

The Ombudsman
FREEPOST
Belfast
BT1 6BR
Freephone 0800 343424

Subject Access

- 5.18 The Data Protection Act 1998 gives individuals the right of 'subject access' and the leaflet *The Data Protection Act 1998: It affects you* tells the Department's customers how the 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 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 the Department's computer systems or any personal information held about them by the Department should write to their local social security office.
- 5.21 Anyone wishing to be provided with information about data on the computer systems of authorities administering Housing Benefit or any personal information held about them should write to their local Housing Executive or Rate Collection Office as appropriate.

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 Social Security Agency's leaflet *GL24 If you think our decision is wrong* explains how to appeal against a decision. This leaflet is available from any social security office or on the Department's website. Authorities administering Housing Benefit will have similar provisions.
- 5.24 This Code of Practice will be reviewed within one year of its initial publication, to ensure that the safeguards and ways in which the law are operated are appropriate and at least once every three years thereafter.

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.