



Department  
for Work &  
Pensions

# Code of Practice on Obtaining Information

Presented to Parliament  
pursuant to section 3 of the Social Security Fraud Act 2001  
November 2016



# Code of Practice on Obtaining Information

Presented to Parliament  
pursuant to section 3 of the Social Security Fraud Act 2001  
November 2016



© Crown Copyright 2016

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit [nationalarchives.gov.uk/doc/open-government-licence/version/3](https://nationalarchives.gov.uk/doc/open-government-licence/version/3) or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: [psi@nationalarchives.gsi.gov.uk](mailto:psi@nationalarchives.gsi.gov.uk).

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

This publication is available at <https://www.gov.uk/government/publications/code-of-practice-on-obtaining-information-social-security-fraud-act-2001>

Any enquiries regarding this publication should be sent to us at

**Bobby Towers**  
**Department for Work and Pensions**  
**Fraud, Error and Debt, Policy and Legislation team**  
**Level 5B Caxton House, Tothill Street**  
**London**  
**SW1H 9NA**

**Email: [robert.towers@dwp.gsi.gov.uk](mailto:robert.towers@dwp.gsi.gov.uk)**

Print ISBN 9781474136297

Web ISBN 9781474136303

ID 11071644 11/16

Printed on paper containing 75% recycled fibre content minimum

Printed in the UK by the Williams Lea Group on behalf of the Controller of Her Majesty's Stationery Office

## Contents

<b>Foreword</b>	<b>4</b>
<b>Chapter 1 Introduction</b>	<b>5</b>
<b>Chapter 2 What are the powers?</b>	<b>8</b>
<b>Chapter 3 Who is authorised to use these powers?</b>	<b>11</b>
<b>Chapter 4 How should the powers be used?</b>	<b>13</b>
<b>Chapter 5 What safeguards are there?</b>	<b>19</b>
<b>Appendix 1 Who can be required to provide information</b>	<b>23</b>
<b>Appendix 2 Examples of the type of information that may be requested</b>	<b>25</b>
<b>Appendix 3 When and about whom may Authorised Officers require Information</b>	<b>26</b>
<b>Appendix 4 Details to be included in requests for information</b>	<b>28</b>
<b>Appendix 5 Contact details</b>	<b>29</b>

### Foreword

- 1 This is version three of the Code of Practice. Version two was issued and laid before Parliament on 30 April 2002.
- 2 The Code has been revised to take account of changes introduced by the Civil Partnership Act 2004, the Welfare Reform Act 2007, the Welfare Reform Act 2012, the Marriage (Same Sex Couples) Act 2013, the Marriage and Civil Partnership (Scotland) Act 2014, Civil Partnership Act 2004 (Consequential Provisions and Modifications) Order 2014 and within the Department for Work and Pensions (DWP) and Other Government Departments more generally.
- 3 DWP has created a Fraud and Error Service, which will enable a single fraud investigation to be undertaken to investigate all social security benefits, including those currently administered by local authorities and His Majesty's Revenue and Customs<sup>1</sup>. The reference to local authority powers in this Code of Practice is relevant whilst individual local authorities still have Authorised Officers undertaking social security benefit fraud investigations. Once a local authority ceases to investigate social security benefit fraud, that local authority Authorised Officer will no longer be bound by this Code of Practice. Local authorities (who still have responsibility for investigating social security fraud) that either have their own Authorised Officers, or use the National Anti-Fraud Network (<http://www.nafn.gov.uk>) for information gathering purposes may still require Information Providers to provide information as set out in this Code of Practice.
- 4 The Investigatory Powers Bill was introduced to the House of Commons in March 2016. Amongst other things, it brings together all of the powers already available to public authorities to obtain communications data. Upon enactment DWPs powers to obtain communications data under Section 109B(2A)(j) of the Social Security Administration Act 1992 (referred to as the Administration Act) will be repealed and new powers to obtain communications data will come into force. At this point, this Code of Practice will no longer apply to the acquisition of communications data.
- 5 Minor changes have also been made to the contact details for the Information Commissioner and Local Government and Public Service Ombudsmen.
- 6 This version will be issued on 21 July 2016.

### 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.

Local Authority and DWP investigators and Authorised Officers should refer to the Fraud Guide for instructions on use of the powers.

<sup>1</sup> See **Appendix 3 (Authorisations for investigations)** for information on the treatment of Tax Credits as social security benefits.

# Introduction

# 1

## What is the purpose of this Code?

- 1.1 The Social Security Fraud Act 2001 (referred to as the Fraud Act 2001) introduced powers for Authorised Officers<sup>2</sup> from the Department for Work and Pensions (DWP) and local authorities<sup>3</sup> to obtain information from specified persons and organisations<sup>4</sup> about their customers to help detect benefit fraud.

More information on the specified list of Information Providers can be found at **Appendix 1**.

- 1.2 The powers were inserted into the Administration Act as amendments to Section 109B and 110A 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. As a statutory code Authorised Officers must have regard to this Code when exercising the powers contained in sections 109B and 110A of the Administration Act. Failure to observe the provisions of the Code does not render a person liable to civil or criminal proceedings however the Code is admissible as evidence in any proceedings in considering if the powers have been used or applied unlawfully. (Unauthorized requests for information are dealt with separately from this Code. See paragraph 1.10 for more information.)
- 1.3 Section 3 of the Fraud Act 2001 (Code of Practice about use of information powers) requires the Secretary of State to issue a Code of Practice detailing the provision and use of the powers.

<sup>2</sup> Authorised Officer has the same meaning as in Part VI of the Administration Act.

<sup>3</sup> Here and elsewhere in the Code the term 'local authority officers' includes those employed by companies sub-contracted by local authorities to undertake the investigation of local authority social security frauds.

<sup>4</sup> In the Code the persons and organisations required to provide information under this legislation are referred to as Information Providers.

## Who is this Code of Practice for?

1.4 This code is intended for:

- DWP authorised officers
- local authority authorised officers (while they still have responsibility for investigating social security benefit fraud)
- organisations and people required to provide information under these powers

The code may also be of interest to persons with a legal interest and members of the public who wish to know more about these powers.

## Who is required to provide information?

1.5 Only those specified in Section 109B(2A) of the Administration Act 1992 may be requested to provide information (a list of Information Providers can be found at **Appendix 1**).

## Who is authorised to request information?

1.6 Only DWP and local authority officers (where that local authority has responsibility for investigating social security benefit fraud) who have undertaken the approved training and are authorised to exercise the powers may make requests for information.

More information about Authorised Officers is contained in **Chapter 3**.

## How should the powers be used?

1.7 To prevent, detect and secure evidence of benefit fraud Authorised Officers may use the powers when it is necessary and proportionate in accordance with relevant legislation.

More information about how the powers should be used is contained in **Chapter 4**. Information Providers can be found at **Appendix 1**.

## What are the safeguards against misuse of the powers?

1.8 Authorised Officers may only request and obtain information, where they are allowed to do so by law. At all times they are obliged to maintain the security and confidentiality of all information that they receive. Information can only be disclosed where it is lawful to do so and in accordance with the relevant legislation.

1.9 Authorised Officers must first consider whether the use of these powers are necessary and that they are the most appropriate to use in order to obtain the required information (see paragraph 4.11).

- 1.10 Authorised Officers, who make unauthorised requests for information, may be liable to civil or criminal proceedings before the courts and subject to disciplinary action by their employers. Authorised Officers (whether still employed or previously employed in social security administration or adjudication) who unlawfully disclose information relating to individuals, acquired in the course of their employment may be liable to prosecution (see Section 123 of the Administration Act).
- 1.11 Comments or complaints about the use of these powers may be made to;
- in the case of DWP, the National Intelligence Leader
  - for local authorities that have responsibility for investigating social security benefit fraud (or its contractors), the fraud manager who made the request. Complaints about a local authority contractor's use of these powers may be raised with the local authority.

More information about how to complain is contained in **Chapter 5**.



# What are the powers?

# 2

## Who can be required to provide information?

- 2.1 Information Providers listed at section 109B(2A) of the Administration Act are legally required to provide information to an Authorised Officer. A list of those Information Providers can be found at Appendix 1.

## What types of information will be requested?

- 2.2 Authorised Officers will request any relevant information necessary for the purposes as set out in Section 109A(2) of the Administration Act. Examples of the type of information that may be requested can be found at **Appendix 2**.
- 2.3 For the purposes of Sections 109A, 109B and 109C of the Administration Act, tax credits (working tax credits and child tax credits) are treated as if they were social security benefits and are therefore subject to those provisions and this code<sup>5</sup>. DWP **Authorised Officers cannot use** the powers of Section 19 of the Tax Credits Act 2002 to enquire about tax credits, instead they must use Section 109A(9) of the Administration Act.
- 2.4 Following an initial response to a request for information, an Authorised Officer may, where it is justified, request information providers to give a more detailed or extensive response.

<sup>5</sup> See **Appendix 3 (Authorisations for investigations)** for information on the treatment of Tax Credits as social security benefits.

## When and about whom may Authorised Officers require information?

- 2.5 Authorised Officers may require information only where they have reasonable grounds for believing that:
- a person (identified by name or description)<sup>6</sup> has committed, is committing or intends to commit a benefit offence
  - a person who is a member of a family of a person who has committed, is committing or intends to commit a benefit offence
  - a person is helping someone else to commit a benefit offence
  - a person is being lied about as part of a benefit claim in respect of them or
  - a fraudulent act against the DWP or local authority has been committed.
- 2.6 DWP Authorised Officers are required to ensure that all requests for information are reasonable (see paragraph 4.11) and specifically for the purposes set out in Section 109A(2) and in the circumstances set out in Section 109B(2C) of the Administration Act. (For Local Authority officers Section 110A(1), 110A(2) and Section 109B(2C) of the Administration Act applies). More information on sections 109A(2), 109B(2C), 110A(1) and 110A(2) of the Administration Act can be found at **Appendix 3**.
- 2.7 Requests will normally seek information about an identified or a named person. Where this is not possible, the Authorised Officer will provide as much information as is available to assist the information provider to identify the person. The Authorised Officer must minimise any risk of obtaining information about innocent third parties. Therefore, if the details provided by the Authorised Officer could relate to more than one particular individual the Information Provider cannot be required to provide any information (see paragraph 2.5).
- 2.8 Authorised Officers may ask for information about people within a family only where their circumstances are directly relevant to the benefit claim being investigated. For example, if a person is claiming an income related benefit but not declaring their partner's earnings, as well enquiring about the claimant, Authorised Officers may make enquiries in relation to the partner's bank account too.
- 2.9 A family is defined in Part 7, Section 137 of the Social Security Contributions and Benefits Act 1992 and associated regulations.
- A family means:
- A couple
  - A couple and a member of the same household for whom one of them is or both are responsible and is a child or a person of a prescribed description.
  - Except in prescribed circumstances, a person who is not a member of a couple and a member of the same household for whom that person is responsible and who is a child or a person of a prescribed description.

<sup>6</sup> Where the name of the suspected fraudster is not known it may be necessary to seek to identify the person by using a description of them and checking this against the address they use. For example, an Authorised Officer may contact a credit reference agency to find out if there is any one particular person matching the suspect's description (e.g. male aged mid-thirties) listed at the address. If there is more than one possible match at that address the Authorised Officer cannot require the credit reference agency to provide any information at all. Authorised Officers must do all they can to eliminate any risk of obtaining information about innocent third parties, which would breach data protection legislation. Neither could an Authorised Officer ask the credit reference company to provide details of all customers living in a block of flats. Enquiries must be necessary in relation to the purposes set out in the legislation.

## 10 What are the powers?

Couple means two people who are:

- married to, or civil partners of, each other and are members of the same household; or
- not married to, or civil partners of, each other but are living together as a married couple otherwise than in prescribed circumstances.

- 2.10 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 that Information Providers supply information if they have been informed that the information is not held or is no longer available. Information Providers are not obliged to inform the Authorised Officer of enquiries that have been made by other law enforcement agencies.
- 2.11 Information that is subject to legal professional privilege or, in Scotland, confidentiality as between client and professional legal adviser will not be requested. Legal professional privilege protects communications between a legal advisor acting in a professional capacity and the client. Providing the communications are confidential and are for the purposes of seeking or giving legal advice the person holding them has no obligation to provide them.
- 2.12 Before an Authorised Officer requests information from an Information Provider (listed at Section 109B(2A) of the Administration Act) consideration must be given as to whether the information could have been obtained directly from the claimant (without jeopardising the investigation). Authorised Officers require full documentation of the steps taken by investigators to seek the information by less intrusive means before requesting information from an information provider. If none have been taken full reasons will be provided by the investigator.

# Who is authorised to use these powers?

# 3

## The Authorised Officer

- 3.1 Only DWP officers who have the Secretary of State's authorisation or local authority officers (where that local authority has responsibility for investigating social security benefit fraud) who have been authorised by their 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 using these powers will be made by Authorised Officers on behalf of fraud investigators. Only staff who have received the appropriate training (see paragraph 1.6) will be eligible for authorisation.
- 3.3 Authorised Officers will hold a certificate of their authority and all Information Providers can access an online list of those officers currently authorised.

## How will officers be authorised?

- 3.4 In DWP, the Senior Intelligence Leader (an officer of Senior Executive Officer grade) acting on behalf of the Secretary of State will authorise officers. Authorised Officers will be of management grade, not below that of Executive Officer. They will be managed by officers not below the grade of Higher Executive Officer.

## 12 Who is authorised to use these powers?

3.5 Local authority staff authorised to use these powers will be of a similar grade. They will be authorised by either:

- 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 in England and Wales), or
- the officer who has responsibility for the authority's financial affairs under Section 95 of the Local Government (Scotland) Act 1973 (in Scotland).

# How should the powers be used?

# 4

## What will Information Providers need to know?

- 4.1 Information Providers should be aware 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 for breach of confidentiality when the request is made in accordance with the law.
- 4.2 Section 35(1) of the Data Protection Act 1998 provides that the disclosure of personal data will not be in contravention of data protection legislation where the disclosure is required by or under any enactment, by any rule of law or by order of the court. Under this provision, Sections 109B and 110A of the Administration Act 1992 contains provisions requiring disclosure of personal information.

## What details should requests for information contain?

- 4.3 Appendix 4 specifies what must be included in all requests for information:

## To whom should enquiries for information be addressed?

- 4.4 The DWP Fraud and Error Service's Central Criminal Intelligence will enter into agreements with Information Providers (listed in Section 109B(2A) of the Administration Act) as to where enquiries should be addressed.

More information on the specified list of Information Providers can be found at **Appendix 1**.

## 14 How should the powers be used?

- 4.5 DWP will maintain a list of Information Providers who have specified a central point of contact for requests. This list will be made available to all Authorised Officers, including local authorities (where the local authority has responsibility for investigating social security benefit fraud).

Requests for information will be made to the organisation care of:

- the nominated central point of contact
- the nominated individual or
- the most senior individual within that organisation that can be identified.

### What happens when an Information Provider fails to provide information?

- 4.6 Information Providers are required to comply with requests within a reasonable time scale. Due to the need to conduct investigations without delay this means within 10 working days although, in exceptional cases, Information Providers may be asked to provide information more urgently.

There may be exceptional situations where an Information Provider is unable to provide the information within 10 working days. In such cases the Information Provider must contact the Authorised Officer to seek a mutually acceptable timescale for providing information. Where multiple requests for information are made to an Information Provider and they are unable to meet the timescale for providing information, a provider liaison point may be set up to negotiate timescales for providing large volumes of information. In these situations Information Providers will not be required to seek changes to timescales on a case by case basis. Action, as detailed in paragraph 4.7, may be taken against Information Providers who fail to provide information within 10 working days and have not made an agreement to extend that deadline.

If an Information Provider is able to provide some but not all of the information within 10 working days, they should do so and agree a timescale with the Authorised Officer for when all of the information will be provided.

- 4.7 An Information Provider who deliberately fails to comply with a written request for information can be prosecuted under Section 111 of the Administration Act. Authorised Officers should inform an Information Provider that they could face criminal proceedings if they refuse to provide the information that has been requested.

- 4.8 It is an offence under Section 111 of the Administration Act to:

- intentionally delay or obstruct an Authorised Officer in their duties or
- refuse or neglect to answer any question or
- fail to furnish any information or produce any document when required to do so by an Authorised Officer.

- 4.9 Information Providers may on conviction, under Section 111 of the Administration Act, be fined up to £1,000 for failing to comply with a request for information. In addition, if after conviction they continue to refuse or neglect to provide the requested information they may be liable on conviction to a fine not exceeding £40 for each day on which they have continued to fail to provide the requested information.

- 4.10 No one is required to provide any information that may incriminate themselves, their spouse or civil partner. No one may be required to provide information subject to legal professional privilege (see paragraph 2.11).

## What reasonable grounds are there for requiring information?

4.11 Authorised Officers can only request the information when there are reasonable grounds for believing that the person to whom it relates (see paragraph 2.5) has committed, is committing or intends to commit a benefit offence. Grounds for requiring information may vary depending on the circumstances of the case and each case must be considered on its own merits.

The Authorised Officer must consider each time if the use of the powers is justified and when deciding whether a request for information should be made Authorised Officers should consider if:

- there is a question that needs an answer for any of the purposes set out in section 109A(2) of the Administration Act.
- the information sought is necessary for any of those purposes
- the use of the powers is a proportionate way of obtaining the information deemed necessary for the purpose, and
- whether the use of the powers is the most appropriate way of obtaining the information, compared to any other method that may be less intrusive but equally effective. This may include obtaining the information from the claimant, but not when to do so would jeopardise the investigation.

4.12 The basic rule is that there must be an objective basis for that belief that is based on facts, information, and/or intelligence which are relevant to the likelihood of obtaining information for any of the purposes set out in section 109A(2) of the Administration Act. Reasonable grounds cannot be supported on the basis of personal factors or a “hunch”.

4.13 Authorised Officers must consider all the facts of the case known to them at that time when deciding what is reasonable. They must ensure that each decision made relating to the use of the powers is documented and available for checking by management or validators. Management checks will ensure that these procedures are followed correctly.

## How will information be requested?

4.14 All requests for information must be made in writing (this can be by post, fax, e-mail or through any other agreed/specified electronic access) with regard to preferences expressed by Information Providers. Requests by email or fax may only be made with prior agreement with the Information Provider.

4.15 Information Providers may reply to requests for information, within 10 working days (unless specified otherwise), in a way 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, however information provided should be in a format that is readily readable. Information Providers who provide information in such a way as to intentionally delay or obstruct an Authorised Officer in their duties may be prosecuted (see paragraph 4.7). Information Providers should take into account any suitable electronic systems available to them when considering the mechanism for providing information. Where information is provided by electronic means, it must be done securely, ensuring an adequate level of protection.



## 16 How should the powers be used?

- 4.16 DWP or local authorities (where the local authority has responsibility for investigating social security benefit fraud) may enter into an agreement with an Information Provider as to how enquiries will be made and the way the information will be provided. Authorised Officers must comply with those arrangements unless there is a specific reason for them not to do so. Authorised Officers should explain to an Information Provider why there is a need to depart from any agreed process. Should a party wish to make a permanent change to an agreed process they should make a formal request to do so and explain their reasons.
- 4.17 DWP should accommodate the views of local authorities (while they still have responsibility for investigating social security benefit fraud) when entering into any arrangement with Information Providers and must advise the local authority of any such agreement reached. Local authorities should comply with any arrangement secured by DWP with Information Providers.
- 4.18 Authorised Officers will not normally make enquiries in person by means of a visit. They may arrange 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 although clarification may be sought in relation to the information already provided.
- 4.19 Authorised Officers will make enquires of specific Information Providers only where they have grounds for believing that they hold information on a particular individual. E.g. Authorised Officers will not normally issue requests to all UK banks asking for information on a particular claimant. However such requests might be required in the most serious cases where the information cannot be obtained by other means. This may only be done in consultation with Fraud and Error Service (Central Criminal Intelligence) or local authority fraud manager (where the local authority has responsibility for investigating social security benefit fraud).

## How will electronic access be managed?

- 4.20 Information held electronically by an Information Provider can be requested by an Authorised Officer.
- 4.21 Only designated Authorised Officers will have access to electronic information with access controlled by passwords or the equivalent. DWP and local authorities will also retain a record of all enquiries in order that this can be cross-checked against their own records.
- 4.22 The Secretary of State and local authorities cannot insist that Information Providers provide them with electronic access to information held if they do not already provide access in this format, or are not able to provide it to another organisation.
- 4.23 In addition, the Secretary of State and local authorities will not require Information Providers to update their computer software in order to provide electronic access. However, DWP and local authorities may enter into arrangements to obtain information electronically where an organisation is already able to provide such access to DWP or another organisation.

- 4.24 The Secretary of State will provide local authorities with information on what is required to enter into arrangements for electronic access. The Secretary of State must be satisfied that a local authority has sufficient controls in place to enable on-line access to be properly monitored and to guard against misuse.
- 4.25 Section 110B of the Administration Act provides local authorities with powers to obtain information electronically. However, they cannot require an Information Provider to enter into arrangements for electronic access or enter into arrangements themselves without the consent of the Secretary of State, which may be granted subject to compliance with particular conditions. Once consent has been obtained from the Secretary of State it may not need to be further obtained each time the local authority wishes to exercise the powers. The local authority must comply with any directions issued in relation to these arrangements. Local authorities do not require consent to enter into arrangements for electronic access to information already available, such as electronic access to an electoral roll.

## How will Authorised Officers manage requests for information?

- 4.26 DWP will ensure that requests for information are made by Authorised Officers within the Fraud and Error Service. Their Central Criminal Intelligence Service will process all enquiries from DWP fraud investigators.
- 4.27 Local authorities (who still have responsibility for investigating Social Security fraud) will take all reasonable steps to limit the number of officers authorised to use these powers, for example, by centralising enquiries within authorities where possible or through the use of the National Anti-Fraud Network to reduce the number of sources from which Information Providers may receive requests for information.
- 4.28 DWP and local authorities will manage requests in such a way as to cause the least amount of inconvenience to the Information Provider and should ensure that the burdens on business are kept to a minimum (see paragraph 4.15).
- 4.29 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. Established security protocols will be agreed with Information Providers, such as passwords, to safeguard the information that is requested.
- 4.30 Information Providers will have access to a secure and up-to-date list of current Authorised Officers. This will be maintained by the Fraud and Error Service, Central Criminal Intelligence Service who will ensure that only current 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 relevant Intelligence Unit, or local authority for further guidance.
- 4.31 All requests for information will include specific details to assure Information Providers that requests received are genuine and who they should deal with if they have any enquiries about the request. See Appendix 4 for details on what will be included in information requests.

## **18** How should the powers be used?

### **How will information be used?**

- 4.32 Any information provided by Information Providers will be treated and evaluated in exactly the same way as information gathered from any other source during a benefit investigation.
- 4.33 In the event that a criminal prosecution is brought for an offence, the information provided by the Information Provider may be used as evidence in criminal proceedings before the courts. Usually this will be in the form of a witness statement or in Scotland a documentary production.

### **Who will receive payment?**

- 4.34 The Secretary of State has the power to make payment to Information Providers in certain circumstances. These providers include:
- credit reference agencies
  - telecommunications companies for specific information such as, reverse telephone number search
  - utilities where we are obtaining bulk information and
  - the servants and agents of the above.
- 4.35 The DWP may where appropriate enter into negotiation with Information Providers in these categories to decide when payment is appropriate and how much will be paid. Local authorities must follow any directions given by the Secretary of State regarding payment for information.

# What safeguards are there?

# 5

## Confidentiality and security

- 5.1 Authorised Officers who obtain information from Information Providers are under a legal duty to observe the rules on confidentiality and must ensure that the information is kept securely and the information is only used for the purpose for which it has been obtained<sup>7</sup>. DWP and local authorities have strict procedures to ensure that:
- information is only used for lawful purposes notified to the Information Commissioner (see paragraph 5.6)
  - access to personal information is limited to those staff who need it to carry out their work and
  - personal information is only disclosed to someone else where it is necessary and lawful to do so.
- 5.2 DWP and local authorities must maintain a record of all access to electronic information using the powers in the Administration Act. This includes undertaking regular audit trails and access checks.
- 5.3 DWP and local authorities will take disciplinary proceedings or other action against members of staff if it is proven that staff have inappropriately accessed or used information that has been provided by an Information Provider. Complaints that are not satisfied through internal management routes are passed for independent scrutiny.

<sup>7</sup> The duty of confidentiality also applies to any DWP employee or contractor who obtains information provided by an Information Provider.

## 20 What safeguards are there?

### The fair and lawful collection of data

- 5.4 DWP and local authorities must process the information that has been provided by the Information Providers lawfully and fairly in order to comply with the provisions contained in the Data Protection Act 1998. The Social Security Administration Act 1992 provides the legislative power to collect and request information from Information Providers.
- 5.5 DWP and local authority claim forms and leaflets inform claimants that information may be sought about them from certain third parties.

### The Information Commissioner

- 5.6 The Information Commissioner is responsible for the promotion of good practice regarding the processing of personal data. He may take action for a breach of the Data Protection Act 1998. Details for the Information Commissioner's offices, where further information can be obtained from can be found at **Appendix 5**.

Further information can be found on the Information Commissioner's Office website at [www.ico.org.uk](http://www.ico.org.uk)

### Penalties for unlawful disclosure

- 5.7 If it appears that Authorised Officers (or any other member of staff, contractor or other person involved in the processing or handling of information provided by an Information Provider) obtained or disclosed information unlawfully, or attempted to do so, they will be subject to an internal and possibly a police investigation. (see paragraph 1.10)

### Retention and storage

- 5.8 Under the Data Protection Act 1998, personal information shall not be kept for longer than is necessary. DWP and local authority staff should follow the guidance provided to them by their organisation.
- 5.9 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 14 months before being destroyed, unless it is required to be retained under the provisions of the Criminal Procedures and Investigation Act 1996, the Criminal Procedure (Scotland) Act 1995, the Regulation of Investigatory Powers (Scotland) Act 2000, the Regulation of Investigatory Powers Act 2000, or for an outstanding appeal or for continuing debt recovery.
- 5.10 When information is obtained, it will be kept in secure storage conditions and may be accessed only by those DWP and local authority staff who have a need to do so, for the purposes of Section 109A(2) of the Administration Act.

## Complaints

- 5.11 Questions about the way that an Authorised Officer has used their powers or the reasonableness of their actions when obtaining information should be referred in the first instance to the Authorised Officer who made the original request.
- 5.12 If this does not provide a satisfactory resolution and the original request for information came from a DWP Authorised Officer the Information Provider should write to the manager of the Intelligence Service Unit. If the complaint is still not resolved, the normal escalation route will be to the National Intelligence Leader.
- 5.13 If a satisfactory outcome still cannot be achieved, the issue will be passed to the Director of the Fraud and Error Service, who will aim to give a full reply within 10 working days.

Director of Fraud and Error Service,  
Department for Work and Pensions,  
Quarry House, Quarry Hill,  
Leeds,  
LS2 7UA.

If a reply cannot be provided within this time, we will say why and advise:

- who is dealing with the letter
  - when a full reply can be expected, and
  - what has been done so far.
- 5.14 Local authorities are independent statutory bodies, each with their own processes for handling complaints about the way in which they operate. 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 which that local authority has in place.
- 5.15 Serious complaints relating to local authority use of electronic access should be addressed to the Chief Executive of the local authority concerned.

## The Parliamentary and Health Service Ombudsman

- 5.16 The Parliamentary and Health Service Ombudsman carries out independent investigations into complaints about unfair or improper actions or poor service by UK government departments and their agencies. Any complaint must be made to a Member of Parliament who will then decide whether to pass the complaint onto the Ombudsman. The Ombudsman seeks to establish whether public bodies have acted correctly and fairly in carrying out their functions and procedures. Contact details of the Parliamentary Ombudsman, where further information can be obtained from, can be found at **Appendix 5**:

Further information can be found on the Parliamentary and Health Service Ombudsman website at **[www.ombudsman.org.uk](http://www.ombudsman.org.uk)**

## 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; each of them deals with complaints from different parts of the country. The Public Service Ombudsmen deals with complaints in Scotland and Wales. Further information can be obtained from the Local Government Ombudsman website: **[www.lgo.org.uk](http://www.lgo.org.uk)** or by writing to them directly. Contact details for the Local Government Ombudsman can be found at **Appendix 5**.

# Appendix 1

## Who can be required to provide information?

Section 109(B)2A sets out the persons who can be required to provide information. They are:

- any bank<sup>8,9</sup> (This includes: banks, credit unions, friendly societies, industrial and provident societies)
- the Director of National Savings
- 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<sup>10</sup> (For example, credit card companies and building societies)
- any insurer<sup>11, 12</sup>
- any credit reference agency (within the meaning given by Section 145(8) of the Consumer Credit Act 1974(c.39))
- 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)
- 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)
- any water undertaker or sewerage undertaker [Scottish Water or any local authority which is to collect charges virtue of an order under section 37 of the Water Industry (Scotland) Act 2002 (asp 3)]

<sup>8</sup> “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 (In this instance an “EEA firm” means a credit institution (as defined in Article 1 of the banking consolidation directive) which is authorised (within the meaning of Article 1) by its home state regulator and does not have its head office in the United Kingdom); 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.

<sup>9</sup> See **Appendix 3 (Authorisations for investigations)** for information on the treatment of Tax Credits as social security benefits.

<sup>10</sup> “credit” includes a cash loan or any form of financial accommodation, including the cashing of a cheque

<sup>11</sup> “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.

<sup>12</sup> 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.



- any person who –
  - is the holder of a licence under Section 7 of the Gas Act 1986 (c.44) to convey gas through pipes, or
  - is the holder of a licence under Section 7A(1) of that Act to supply gas through pipes
- any person who (within the meaning of the Electricity Act 1989(c.29)) distributes or supplies electricity
- any person who provides a telecommunications service<sup>13, 14</sup>
- any person conducting any educational establishment or institution
- any body the principal activity of which is to provide services in connection with admissions to educational establishments or institutions
- the Student Loans Company
- any servant or agent of any person mentioned in any of the preceding paragraphs.

<sup>13</sup> “telecommunications service” has the same meaning as in the Regulation of Investigatory Powers Act 2000 (c. 23) which states that “telecommunications service” means any service that consists in the provision of access to, and of facilities for making use of, any telecommunication system (whether or not one provided by the person providing the service)

<sup>14</sup> This only applies while DWP has powers under Section 109B(2A)(j) of the Administration Act to obtain communications data. These powers are to be repealed by the Investigatory Powers Bill 2016.

## Appendix 2

# Examples of the type of information that Authorised Officers may request

- bank statements
- building society statements
- details of income from an insurance policy
- address records from a credit reference agency
- customer details from a utility company
- student status from the Student Loan Company
- mortgage application details
- telephone subscriber and account details
- identity of internet service provider and subscriber.<sup>15</sup>

This list is not exhaustive.

<sup>15</sup> Telephone and internet subscriber and provider information may only be requested while DWP has powers under Section 109B(2A)(j) of the Administration Act to obtain communications data. These powers are to be repealed by the Investigatory Powers Bill 2016.

## Appendix 3

# When and about whom may Authorised Officers require information?

Paragraph 2.4 of this Code explains that requests for information must be reasonable and must be made specifically in accordance with the legislation.

**Section 109A(2)** of the Administration Act sets out the purposes whereby an Authorised Officer may request information. 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.

**Section 109B(2C)** of the Administration Act explains when an Authorised Officer may require an information provider (as detailed in section 109B(2A)) to provide information.

An authorised officer shall not, in exercise of those powers, require any information from any person by virtue of his falling within subsection (2A) above unless it appears to that officer that there are reasonable grounds for believing that the identified person to whom it relates is–

- (a) a person who has committed, is committing or intends to commit a benefit offence; or
- (b) a person who (within the meaning of Part 7 of the Contributions and Benefits Act) is a member of the family of a person falling within paragraph (a) above.

## Authorisations for investigations

Section 122(2) of the Welfare Reform Act 2012 inserted Section 109A(9) into the Administration Act, providing for Working Tax Credits and Child Tax Credits to be treated as social security benefits for the purposes of sections 109A to 109C of the Administration Act.

**Section 109A(9)** says:

This section [*i.e.* section 109A] and sections 109B to 109C below apply as if –

- (a) the Tax Credits Act 2001 were relevant social security legislation, and
- (b) accordingly, child tax credit and working tax credit were relevant social security benefits for the purposes of the definition of “benefit offence”.

**Section 110A – (1)** says that:

An individual who for the time being has the authorisation for the purposes of this Part of an authority administering housing benefit or council tax benefit (“a local authority authorisation”) shall be entitled, for a relevant purpose, to exercise any of the powers which, subject to subsection (8) below, are conferred on an authorised officer by sections 109B and 109C above.

(1A) Each of the following is a relevant purpose.

- (a) a purpose mentioned in subsection (2) below;
- (b) a purpose mentioned in section 109A(2)(a), (c) or (d).

(1B) If the Secretary of State prescribes conditions for the purposes of this section, an authority must not proceed under this section for a purpose mentioned in section 109A(2)(a), (c) or (d) unless any such condition is satisfied.

(1C) An authorisation made for a purpose mentioned in section 109A(2)(a), (c) or (d)–

- (a) is subject to such restrictions as may be prescribed;
- (b) is not valid in such circumstances as may be prescribed.

**Section 110A (2)** purposes 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);
- (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.

**Section 109B (2C)** is as above.

## Appendix 4

# Details to be provided by Authorised Officers when requesting information

All requests for information will include the following details:

- the name and contact number of the Authorised Officer making the request
- a copy of the Authorised Officers certificate
- the name of the Intelligence Unit Manager or local authority Fraud Manager
- the address where the information must be sent to, and
- sufficient information to ensure that the customer, and the particular account in question, can be identified.

Requests for information may also include details such as:

- the customers date of birth
- the customers address
- a description of the customer and
- any customer reference numbers.

## Appendix 5

# Contact details

### Ombudsman's Offices

#### **The Parliamentary and Health Service Ombudsman**

Millbank Tower  
Millbank  
London, SW1P 4QP

#### **England:**

The Local Government Ombudsman  
PO Box 4771  
Coventry, CV4 0EH

#### **Scotland:**

Scottish Public Services Ombudsman  
4 Melville Street  
Edinburgh, EH3 7NS

#### **Wales:**

Public Services Ombudsman for Wales  
1 Ffordd yr Hen Gae  
Pencoed, CF35 5LJ

### Information Commissioner's Offices

#### **England:**

The Information Commissioner's Office  
Wycliffe House  
Water Lane  
Wilmslow  
Cheshire, SK9 5AF

#### **Scotland:**

Information Commissioner's Office – Scotland  
45 Melville Street  
Edinburgh, EH3 7HL  
Telephone: 0131 244 9001  
Email: [Scotland@ico.org.uk](mailto:Scotland@ico.org.uk)

#### **Wales:**

Information Commissioner's Office – Wales  
2nd Floor  
Churchill House  
Churchill Way  
Cardiff, CF10 2HH  
Telephone: 029 2067 8400  
Fax: 029 2067 8399  
Email: [wales@ico.org.uk](mailto:wales@ico.org.uk)

This publication can be accessed online at:  
[https://www.gov.uk/government/publications/  
code-of-practice-on-obtaining-information-  
social-security-fraud-act-2001](https://www.gov.uk/government/publications/code-of-practice-on-obtaining-information-social-security-fraud-act-2001)

For more information about this publication,  
contact:

**Bobby Towers**  
**Department for Work and Pensions**  
**Fraud, Error and Debt,**  
**Policy and Legislation team**  
**Level 5B Caxton House,**  
**Tothill Street**  
**London**  
**SW1H 9NA**

**Email: [robert.towers@dwp.gsi.gov.uk](mailto:robert.towers@dwp.gsi.gov.uk)**

Copies of this publication can be made  
available in alternative formats if required.

Department for Work and Pensions  
November 2016  
[www.gov.uk](http://www.gov.uk)

