DWP Obtaining Information to Support Fraud Investigations in the Welfare System Code of Practice [DRAFT]

Contents

Disclaimer

This is a draft of the Obtaining Information to Support Fraud Investigations in the Welfare System Code of Practice. The Code will be laid in Parliament and issued once the relevant provisions come into force.

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, the law, or any obligations or responsibilities you may have, you should seek independent advice.

This Code applies once the relevant provisions in the Public Authority (Fraud, Error and Recovery) Act 2025 come into force.

Foreword

1. This is version four of the Code of Practice ("Code"). A previous version was issued and laid before Parliament on 21 July 2016.

2. This Code of Practice ("Code") is authorised under Section 3 of the Social Security Fraud Act 2001 which requires the Secretary of State to issue a Code of Practice about the use of information powers and information notices under Section 109BZA of the Social Security Administration Act 1992.

3. The Code has been revised to take account of changes introduced by the Public Authorities (Fraud, Error and Recovery) Act 2025. The amendments introduced by the 2025 Act modernise the existing powers held by Department for Work and Pensions (DWP) to enable Authorised Officers to obtain information from any relevant Information Provider to support fraud investigations, subject to exemptions for certain types of information. This changes the approach from DWP having a list of organisations and people who can be compelled to provide information, to a power to require the provision of relevant information from 'any person', with specific exemptions for certain types of information.

4. All investigations into social security fraud under this Code are carried out solely by DWP Authorised Officers.

5. Investigations will undergo inspections by His Majesty's Inspectorate of Constabulary and Fire and Rescue Services (HMICFRS), as well as His Majesty's Inspectorate of Constabulary (HMICS) in Scotland, who may be commissioned to examine the end-to-end criminal investigations process.

6. If substantive revisions are required to this Code, the Secretary of State must hold a Public Consultation on the new draft and lay the new Code before Parliament.

1. Introduction

What is the purpose of this Code?

1.1 The Public Authorities (Fraud, Error and Recovery) Act 2025 inserted the powers into the Social Security Administration Act 1992 to allow DWP Authorised Officers authorised by the Secretary of State to require information about suspected fraud. This Code governs the use of these powers by Authorised Officers within DWP. Authorised Officers must have regard to this statutory Code when exercising the powers contained in Section 109BZA of the Social Security Administration Act 1992. Failure to observe the Code does not in itself render a person liable to civil or criminal proceedings. However, the Code is admissible as evidence in any proceedings where the manner in which these powers have been exercised is in question. Unauthorised requests for information are dealt with separately from this Code.

1.2 Fraud does occur in the welfare system, committed both by individuals and organised criminals. Where a suspicion of fraud arises, the DWP has legal powers to investigate to prove or disprove the allegation. These powers are set out in the Social Security Administration Act 1992 and the Social Security Fraud Act 2001, as amended. These powers are limited to specified staff known

as “Authorised Officers” who work within criminal investigation teams.

1.3 Gathering information is an important stage in investigating a fraud allegation. The same legislation sets out how information can be compelled by Authorised Officers. It also sets out the exemptions and limitations on when information can be compelled – including that there must be a suspicion of fraud relating to an identifiable individual (by name or description); the information must be information that the Information Provider is reasonably expected to hold; and it must be necessary and proportionate to require it for the purposes of the investigation.

1.4 Section 3 of the Social Security Fraud Act 2001 requires the Secretary of State to issue a Code of Practice detailing the provision and use of DWP’s modernised powers to obtain information in cases of suspected fraud from any person, subject to exemptions for certain types of information. This document fulfils that requirement.

Who is this Code for?

1.5 This Code is intended for:

(i) DWP Authorised Officers responsible for requesting information under these powers,

(ii) Information Providers required to provide information under these powers.

1.6 Only DWP Authorised Officers, authorised by the Secretary of State for investigating a DWP offence under Section 109A(1), may exercise the powers set out in this Code. Subsections 2(c) and (d) of Section 109A of the Social Security Administration Act 1992 set out the purposes for which these powers can be exercised. Authorised Officers will be trained and accredited and issued with a certificate of their authority to act. On receipt of an information notice, this authorisation will be made clear to an Information Provider (a third-party obliged to provide information to DWP following receipt of an information notice) to show that this is a genuine request sent by an Authorised Officer.

1.7 More information about Authorised Officers is contained in **Chapter 2**.

Who is required to provide information?

1.8 Authorised Officers may issue an information notice to a person or organisation under Section 109BZA of the Social Security Administration Act 1992, when they have reasonable grounds to suspect that a person has committed, is committing, or intends to commit a DWP offence. A DWP offence, as defined in section 121DA (Social Security Administration Act 1992) includes any offence related to a DWP benefit or grant, and

an offence related to the allocation or use of a National Insurance Number.

1.9 Section 109BZA enables DWP Authorised Officers to issue information notices to any person or organisation that they believe may hold relevant information in respect of a criminal investigation into a DWP offence, unless the information is exempt. Should an Information Provider not have access to the information requested or be unable to provide it for some other reason, they must inform the DWP as to why they cannot comply with the information notice. DWP may contact the organisation to discuss those reasons and determine whether any further action will be taken.

1.10 Certain exemptions apply to DWP's information gathering powers which are set out in the legislation and further detail is provided at Appendix 1. An Authorised Officer cannot compel an Information Provider to provide:

- Information that is subject to legal professional privilege or, in Scotland, information held in confidence between a client and their professional legal adviser.
- Information which may incriminate the holder of that information, or their spouse or civil partner.
- Personal information about the recipients of services provided on a free of charge basis in relation to social security, housing (including

the provision of free accommodation) or debt. These types of services include free advice, advocacy and crisis support. For example, if a person is seeking support from a domestic abuse charity, DWP cannot request personal information from the charity about that person.

- Information that is defined as 'journalistic material' and 'excluded material' under Sections 11 to 13 of the Police and Criminal Evidence Act 1984 (PACE). This includes personal records pertaining to a person's physical and mental health.

1.11 In the event that an Authorised Officer requests information, in good faith, that the Information Provider believes falls under one or more of the above exemptions, the Information Provider should inform the DWP that they believe the information requested is exempt.

1.12 These powers do not authorise any processing of information that contravenes data protection legislation (as defined in section 3(9) of the Data Protection Act 2018) or information that is prohibited by any of Parts 1 to 7 or Chapter 1 of Part 9 of the Investigatory Powers Act 2016 which covers provisions related to obtaining communications data.

How should the powers be used?

1.13 All cases are dealt with on an individual basis and ‘reasonable suspicion’ must be formed for each case before it becomes a criminal investigation and is subject to DWP’s information gathering powers. Reasonable suspicion means that an Authorised Officer holds an objective belief that a DWP offence has been, is being, or is going to be, committed, and that belief must be based on facts and information. Where an Authorised Officer has a reasonable suspicion, they may only request information where it is necessary, reasonable and proportionate to do so.

1.14 The information that is requested will vary and is dependent on each case and the type of alleged fraud. For example, where there is an income related fraud investigation, it may be relevant and proportionate for the Authorised Officer to make an information request to the suspect’s employer to confirm their salary to prove or disprove fraud. The information notice will set out what information is being sought and must be about a named or identifiable individual. See paragraphs 3.2 to 3.7 for further information.

1.15 Authorised Officers must only request information that is clearly relevant to the investigation – for example, where there is a suspicion that someone is working but has not declared it, an Authorised Officer may request bank statements

to determine if they are being paid wages. The power under Section 109BZA of the Social Security Administration Act 1992 does not allow DWP to request information without a clear, necessary and proportionate reason to do so. Authorised Officers must be able to explain why the request is needed for one or both of the purposes in Section 109A(2)(c) and (d) and record their reasoning. See paragraph 3.2(i) and (ii) for further information.

1.16 Authorised Officers must have regard to all relevant information that is held by DWP when deciding whether to issue an information notice. This means, for instance, considering all information DWP holds that is relevant to assessing whether there are reasonable grounds to suspect a DWP offence or whether the information notice is necessary and proportionate. Authorised Officers should also be aware that where information received via DWP's Eligibility Verification Measure (EVM) is relevant to the decision about whether to issue the information notice, this requirement to consider all other relevant information is also set out in the legislation (see Schedule 3B paragraph 5(2) and (3) of the Social Security Administration Act 1992). For more information on EVM, please see the relevant Code of Practice on Eligibility Verification Notices.

What are the safeguards against misuse of the powers?

1.17 Authorised Officers may only request, obtain and retain information where they are allowed to do so under the relevant provisions in the Social Security Administration Act 1992 and must abide by obligations set out under the relevant data protection legislation. At all times they must follow Departmental guidelines to ensure that all information obtained is kept and dealt with securely and confidentially.

1.18 Before issuing an information notice, Authorised Officers must first consider whether the use of the power is necessary, whether an information notice is the most appropriate way to obtain the required information and whether the information can be obtained in a less intrusive manner. For example, when investigating income related fraud, the Authorised Officer should first determine if DWP already has access to that information through existing DWP records before making a request to a bank.

1.19 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 DWP. 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 Social Security Administration Act 1992).

1.20 There are internal and external processes for complaints to be made about the use of these powers. See **Chapter 6** for further information. See **paragraph 6.1** for further information on independent inspections by His Majesty's Inspectorate of Constabulary and Fire and Rescue Services (HMICFRS).

2. Who is authorised to use these powers?

The Authorised Officer

2.1 Only DWP officers who have the Secretary of State's authorisation may use these powers. These officers are known as Authorised Officers.

2.2 Only staff who have received the appropriate training (see **paragraph 2.5**) will be eligible for authorisation.

2.3 Authorised Officers will hold a certificate of their authority which Information Providers will be made aware of when a request is made.

How will officers be authorised?

2.4 In DWP, the Senior Leader (an officer of Senior Executive Officer grade) acting on behalf of the Secretary of State will authorise officers.

2.5 Alongside internal training provided by DWP, individuals must complete an accredited counter fraud programme and become members of the Government Counter Fraud Profession[1] before they can be authorised to use these powers.

---

1 See **Government Counter Fraud Function and Profession - GOV.UK**

2.6 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.

What are the powers?

2.7 Authorised Officers can only issue an information notice when there are reasonable grounds for suspecting that a person has committed, is committing, or intends to commit a DWP offence. Reasonable grounds for suspicion may vary depending on the circumstances of the case and each case must be considered on its own merits.

3. What are the powers?

3.1 Authorised Officers can only issue an information notice when there are reasonable grounds for suspecting that a person has committed, is committing, or intends to commit a DWP offence. Reasonable grounds for suspicion may vary depending on the circumstances of the case and each case must be considered on its own merits.

How will Authorised Officers determine a reasonable suspicion of fraud?

3.2 As set out in the legislation an Authorised Officer must ensure that they have reasonable grounds to suspect a DWP offence before issuing an information notice. Authorised Officers must take care not to rely on grounds that are arbitrary, discriminatory, or lacking proper evidence base, and each case must be considered on its own merit and the facts which relate to the fraud allegation. This reasonableness test must be applied to the particular circumstances in each case and is in two parts:

(i) First, the Authorised Officer must have formed a genuine suspicion in their own mind that a person has committed, is committing, or intends to commit a DWP offence; and

(ii) Secondly, the suspicion that a person has committed, is committing, or intends to commit a DWP offence must be reasonable. This means that there must be an objective basis for that suspicion based on facts, information and/or intelligence which are relevant to the likelihood of such an offence, and that a reasonable person would be entitled to reach the same conclusion based on the same facts and information and/or intelligence.

3.3 Therefore, reasonable grounds can never be supported on the basis of a “hunch”. Personal factors can also never support reasonable grounds for suspicion, for instance any assumption that specific groups are more likely to commit fraudulent acts such as generalisations or stereotypes about individuals (e.g. based on nationality, race, income or background).

3.4 Authorised Officers must ensure that each decision made relating to the use of the powers can be explained, is documented (including how and why the decision was reached) and available for routine checking by management and any inspection body. Management checks will ensure that these procedures are followed correctly and quality-assure adherence with these standards.

How will Authorised Officers determine what is necessary and proportionate

3.5 The legislation requires that an Authorised Officer must consider that requiring the information set out in the information notice is necessary and proportionate for the purposes set out in section 109A(2)(c) or (d) of the 1992 Act before issuing the information notice.

3.6 In considering this, an Authorised Officer should have regard to, among other things, the particular facts of the case; the information that constituted a reasonable suspicion of fraud; the nature of the suspected offence; the specific information provider being asked to provide the information; how the information may assist in proving or disproving the relevant suspicion; and the precise nature and volume of information being requested. Officers should ensure that the request is limited to information that is relevant to the period to which the suspicion relates to and specific to the particular case under investigation.

3.7 Regard should also be had to whether the use of the powers is necessary in the sense of whether the information could be obtained through any less intrusive means (as explained in paragraph 3.16).

When may Authorised Officers require information and about whom?

3.8 As above, Authorised Officers may require information only where they have reasonable grounds for believing that a person has committed, is committing or intends to commit, a DWP offence. That person must be identified by name or description in the information notice or be a member of that person's family (as explained in paragraph 3.12).

3.9 Legislation defines a DWP offence (see section 89 of the Public Authorities (Fraud, Error and Recovery) Act 2025 which inserts the definition into section 121DA of the Social Security Administration Act 1992) as including any offence pertaining to a benefit or grant for which DWP has responsibility. It also includes attempts and conspiracies to commit such offences. This means an Authorised Officer may have reasonable grounds to suspect a DWP offence is being committed where they suspect that a person is helping someone else to commit a DWP offence.

3.10 Information notices must be in relation to an identifiable person either by name or description. Where it is not possible to name someone, the Authorised Officer will provide information to assist

the Information Provider to identify the person[2]. The Authorised Officer must minimise any risk of obtaining irrelevant information about other people by providing as much necessary detail as possible to enable the Information Provider to identify the individual who is the subject of an information notice.

3.11 Authorised Officers may require 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 as

---

2 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 irrelevant information about other people, which would breach data protection legislation. Enquiries must be necessary in relation to the purposes set out in the legislation.

enquiring about the claimant, Authorised Officers may make enquiries in relation to the partner's bank account too.

3.12 A family is defined in Part 7, Section 137 of the Social Security Contributions and Benefits Act 1992 and associated regulations. This sets out that a family includes:

- A couple;
- A couple and a member of the same household for whom one or both are responsible, and who is a child or a person of a prescribed description;
- Except in certain circumstances, where a person (who is not a member of a couple) and a child (or person of a prescribed description) who is a member of their household for whom they are responsible.

3.13 A 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.

3.14 Authorised Officers may only require information that they have reasonable grounds to suspect the Information Provider holds or has access to. This means that the information that is requested will

normally be information that they keep as part of their normal business. Authorised Officers cannot insist that Information Providers supply information if they have been informed that it 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.

3.15 Obtaining information that is subject to legal professional privilege or, in Scotland, confidentiality as between client and professional legal adviser is legally prohibited and must not be requested. Legal professional privilege protects communications between a legal advisor acting in a professional capacity and the client. Where 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.

3.16 Before an Authorised Officer requests information from an Information Provider, consideration must be given as to whether the information could be obtained less intrusively, for example via DWP internal systems. Authorised Officers are required to fully document the steps they have taken using internal guidance templates to seek the information by less intrusive means before requesting information from an Information Provider. If the information cannot be obtained through less intrusive means, the investigator must provide a

reason why. These records must be retained for audit and inspection purposes.

3.17 Subject to the exemptions above, Authorised Officers may request any relevant information where it is necessary, proportionate and relevant to investigate suspected DWP offences. These are the purposes set out in Section 109BZA. Examples of the type of information that may be requested can be found at **Appendix 2**.

To whom should enquiries for information be addressed?

3.18 Following an initial response to a request for information, an Authorised Officer may, where it is justified, request Information Providers give a more detailed or extensive response.

3.19 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.

3.20 Requests for information will be made to the Information Provider for the attention of:

- The nominated central point of contact;
- The nominated individual; or
- The most senior individual that can be identified.

3.21 The DWP will instruct Information Providers as to where enquiries should be addressed.

3.22 DWP Authorised Officers will issue an information notice to the relevant Information Provider which will set out the requirements for the Information Provider to comply with and consequences for not complying. The notice must specify or describe:

- The identity of the person to whom the information requested relates;
- When the information notice must be complied with; and
- How the information notice must be complied with (digitally unless specified otherwise in the notice).

3.23 Information Providers must comply with those arrangements unless there is a specific reason for them not to do so.

3.24 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.

How will Authorised Officers manage requests for information?

3.25 DWP will ensure that requests for information are made by Authorised Officers who are permitted to use these powers. **Paragraph 5.4** of this Code provides further details on the safeguards in place to prevent misuse of these powers by DWP Authorised Officers and outlines the consequences of such misuse. To prevent unauthorised access or impersonation, requests will be made primarily by digital means, which will restrict access to issuing an information notice to only DWP Authorised Officers.

3.26 DWP will seek to manage requests in such a way as to cause the least inconvenience to the Information Provider and should ensure that the burdens on business are kept to a minimum.

3.27 DWP will make sure that adequate provisions are in place to ensure that requests for information are made and received securely through digital means.

3.28 Information Providers will have access to the credentials of the Authorised Officer who made the request for information. If a request is received by an officer who has not provided their credentials, then it should be refused, and the Information Provider should contact DWP for further guidance (see Chapter 6: Internal complaints process for contact details).

What happens if an Information Provider fails to provide information?

3.29 Information Providers are required to comply with requests within a reasonable time scale. The time scale will be specified in the information notice. Due to the need to conduct investigations without delay, this will normally be within 10 working days unless specified otherwise. In exceptional cases, Information Providers may be asked to provide information more urgently.

3.30 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 the requested information. Where multiple requests for information are made to an Information Provider and they are unable to meet the timescale for providing the information, a provider liaison point may be set up to negotiate timescales. In these situations, Information Providers will not be required to seek changes to timescales on a case-by-case basis. Legal action may be taken against Information Providers who fail to provide information within the specified timeframe and have not made an agreement to extend that deadline.

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

3.32 If an Information Provider is not able to comply with an Information Notice, they must inform the Authorised Officer who made the request and provide an explanation setting out their reasons. The Authorised Officer will consider if this explanation is reasonable, for example, if an Information Notice is requesting information that the Information Provider believes is exempt.

3.33 An Information Provider who deliberately fails to comply with a written request for information can be prosecuted under Section 111 of the 1992 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.

3.34 It is an offence under Section 111 of the Social Security Administration Act 1992 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.

3.35 Information Providers may on conviction, under Section 111 of the Social Security Administration Act 1992, 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.

3.36 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.

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 by an Authorised Officer. This obligation overrides any duty of customer confidentiality and means that they cannot be held liable for breach of confidentiality when the request is made in accordance with the law.

4.2 **Appendix 3** specifies what must be included in all requests for information.

Who will receive payment?

4.3 The Secretary of State can make payment arrangements in respect of the provision of information where the Secretary of State considers it appropriate. The DWP may, where it thinks fit, enter into negotiation with Information Providers to decide whether payment is appropriate and if so, how much will be paid.

4.4 DWP intends that this will only apply in cases where the provision of information for payment is the sole (or principle) purposes of that business (e.g., Credit Reference Agencies who often charge third parties to share data), though there may be other circumstances where the Secretary of State decides payment arrangements are appropriate.

How will information be used?

4.5 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.

Confidentiality and security

4.6 Authorised Officers who obtain information from Information Providers are under a legal duty to observe the rules on confidentiality in internal guidance and must ensure that the information is kept securely, and the information is only used for the purpose for which it has been obtained. DWP have strict procedures to ensure that:

- Information is only used for lawful purposes;
- 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.

4.7 DWP must maintain a record of all information notices made and information received by Authorised Officers under Sections 109BZA and 109BA of the Social Security Administration Act 1992. Records of information notices issued

and information received will be kept by DWP, supporting and maintaining a clear audit trail of their use of these powers. Where provided digitally, this will help ensure the records are clear and accessible.

4.8 DWP will take disciplinary proceedings or other action against members of staff if it is proven that they have inappropriately accessed or used information that has been provided by an Information Provider. Complaints that are not satisfied through internal management routes can be passed for independent scrutiny where Information Providers can raise a complaint which will be sent to the Independent Case Examiner before being referred to the Parliamentary Health and Services Ombudsman and the Information Commissioners Office (see **paragraphs 6.2, 6.10** and **Appendix 4** for further information).

5. The fair and lawful collection of data

5.1 DWP must process the information that has been provided by the Information Providers lawfully and fairly, complying with data protection legislation. The Social Security Administration Act 1992 provides the legislative power to require the information from Information Providers.

5.2 DWP claim forms and leaflets inform claimants of the circumstances that information may be sought about them from certain third parties.

5.3 More detailed information about data retention is available in various public places, including the Personal Information Charter (**Personal information charter - Department for Work and Pensions - GOV.UK**) and DWP information management policies (**DWP: information management policies - GOV.UK**).

Penalties for unlawful disclosure

5.4 If it appears that Authorised Officers obtained or disclosed information unlawfully, or attempted to do so, they will be subject to an internal investigation.

Retention and storage

5.5 Data protection legislation requires that personal information must not be kept for longer than is necessary. DWP staff should follow all relevant internal guidance.

5.6 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 24 months before being destroyed, unless longer retention is required under the Criminal Procedures and Investigations 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 Proceeds of Crime Act 2002 asset recovery.

5.7 When information is obtained, it will be kept in secure storage conditions and may be accessed only by those DWP staff who have a need to do so for the purposes of a fraud investigation under Section 109A(2)(c) and (d) of the Social Security Administration Act 1992.

6. Complaints and Oversight

6.1 DWP have commissioned an “independent person/ body”, His Majesty’s Inspectorate of Constabulary and Fire and Rescue services (HMICFRS) and His Majesty’s Inspectorate in Scotland (HMICS) to carry out reviews by virtue of Section 89 of the Public Authorities (Fraud, Error and Recovery) Act 2025. An independent inspection may review all functions exercised within a criminal investigation. This review will form a key oversight function for DWP criminal investigations, where these information gathering powers will be in scope.

The Information Commissioner’s Office (ICO)

6.2 The ICO is responsible for regulating data protection law and upholding data rights in the public interest. They may take action against organisations for a breach of the law. Individuals can also complain to the ICO where they are unhappy with how an organisation has used their personal information.

6.3 Further information can be found on the Information Commissioner’s Office website at **www.ico.org.uk**.

Internal Complaints Process

6.4 Questions about the way that an Authorised Officer has used their powers or the reasonableness of their actions when obtaining information should be referred to the Authorised Officer in the first instance, who made the original request.

6.5 If this does not provide a satisfactory resolution then the Information Provider should write to the manager of the Intelligence Unit. If the complaint is still not resolved, the normal escalation route will be to the Operational Intelligence Unit Senior Intelligence Leader.

6.6 If a satisfactory outcome still cannot be achieved, the issue will be passed to the **Director of Counter Fraud, Compliance and Debt**, who will aim to give a full reply within 10 working days.

6.7 If it appears that Authorised Officers obtained or disclosed information unlawfully, or attempted to do so, they will be subject to an internal and possibly a police investigation.

6.8 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.

6.9 Serious complaints relating to DWP Authorised Officers should be addressed to the Director of Counter Fraud, Compliance and Debt.

External Complaints Process

Parliamentary and Health Service Ombudsman

6.10 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 4**.

6.11 Further information can be found on the Parliamentary and Health Service Ombudsman website at **www.ombudsman.org.uk**.

Vulnerability

6.12 DWP have existing processes in place when dealing with vulnerable claimants at each stage of a fraud investigation. When gathering information for fraud purposes, Authorised Officers must

consider whether the subject is identified as having 'complex needs'.

6.13 The Investigator must, at all times, balance the needs and safety of the individual against the public interest for the case to proceed. Authorised Officers are able to refer a case to a Vulnerable Customer Champions and Advanced Customer Support Leaders who are designated to provide advice on avenues of assistance that can be offered to an individual at any point in the investigation.

6.14 Investigators must also adhere to the DWP Customer Charter, which includes commitments to treat people fairly, understand people's circumstances and explain things clearly. The full Customer Charter is available at **http://www.gov.uk/government/publications/our-customer-charter/our-customer-charter**.

6.15 The Equality Act 2010 also places obligations on DWP to make reasonable adjustments for vulnerable claimants or their representatives where necessary.

7. Appendices

Appendix 1: Exemptions

Under this legislation DWP can request information from any Information Provider where there is a reasonable suspicion of fraud and it is necessary and proportionate to make such a request. The exercise of these powers must comply with obligations set out in the Data Protection Act 2018.

There are some exemptions that apply to this compulsion, which are:

- Information that relates to legal professional privilege which protects confidential communication between a lawyer and their client from disclosure. The same applies in Scotland.
- Self-Incrimination: Information that could potentially implicate an individual, or their spouse or civil partner, in wrongdoing.
- Personal information about the recipients of services provided on a free of charge basis in relation to social security, housing (including the provision of free accommodation) or debt. These types of services include free advice, advocacy and crisis support. For example, if a person is seeking support from a domestic abuse charity, DWP cannot request personal information from the charity about that person.

- Information that is defined as ‘journalistic material’ and ‘excluded material’ as defined under Section 11 to 13 of the Police and Criminal Evidence Act 1984 (PACE) must not be requested. This includes certain types of information, including personal records relating to physical or mental health, spiritual counselling or assistance, journalistic material held in confidence, human tissue and tissue fluid.
- Any information that has been identified as communications data, for example subscriber information, phone numbers, or IP addresses, may not be requested using these powers[3].

3 See Part 3 of the Investigatory Powers Act 2016: **Investigatory Powers Act 2016**

Appendix 2: Types of Information which can be requested

This list provides examples and is not exhaustive. Information that may be requested could include:

- 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.

Appendix 3: 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 Officer's certificate,
- The name of the Operational Intelligence Unit Senior Intelligence Manager,
- Sufficient information to ensure that the customer, and the particular account in question for example, are identifiable.

Requests for information must also include details such as:

- The name of the individual,
- Their date of birth,
- Their address,
- A description of the individual,
- Any reference numbers associated with them.

All information notices must include the following, as required by Section 109BZA(4) of the Social Security Administration Act 1992:

- How the information is to be provided (e.g. format or method),
- Where the information must be sent,
- When the information must be provided by (i.e. a specific deadline),
- The potential consequences of failing to comply.

Appendix 4: Contact details

Ombudsman's Offices

England	The Parliamentary and Health Service Ombudsman Citygate, Mosley Street Manchester, M2 3HQ
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 – England Wycliffe House, Water Lane Wilmslow, Cheshire, SK9 5AF Telephone: 0303 123 1113 Fax: 01625 524510
Scotland	Information Commissioner's Office – Scotland 6th floor, Quartermile One, 15 Lauriston Place Edinburgh, EH3 9EP Telephone: 0303 123 1115 Email: Scotland@ico.org.uk
Wales	Information Commissioner's Office – Wales 2nd Floor Churchill House, Churchill Way Cardiff, CF10 2HH Telephone: 0330 414 6421 Email: wales@ico.org.uk

Appendix 5: Key Terms and Definitions

Authorised Officer	A DWP official accredited by the Secretary of State who received appropriate training and authorisation to issue information notices and conduct investigations.
Information Provider	Any person or organisation, such as banks or employers, that possesses information relevant to a DWP fraud investigation. This will never include the person who is suspected of an offence.
Information Notice	A request for information issued by a DWP Authorised Officer compelling an Information Provider to provide specific information for the purposes of investigating fraud.
Reasonable grounds	An objective view requiring specific evidence that would lead a DWP Authorised Officer to suspect that fraud has occurred.
Oversight	The means of monitoring and reviewing DWP's use of its information gathering powers to ensure compliance with the legislation.
Necessity	A requirement that the information must be needed to achieve the purpose for which it is requested.

Proportionality	Ensuring the level of intrusion is balanced against the importance of the aim, and that no more information is requested than is needed.
Excluded Material	This is defined under Section 11 of the Police and Criminal Evidence Act 1984 (PACE)and includes information such as personal records relating to a person's physical or mental health, confidential journalistic material, or human tissue held for medical purposes. This information is exempt from disclosure under the information gathering powers described in this Code.
Data protection legislation	As set out in section 3(9) of the Data Protection Act 2018, this includes the Data Protection Act 2018, UK GDPR, and associated regulations.