**Code of practice on obtaining information in relation to
The Council Tax Reduction Schemes (Detection of Fraud and Enforcement) (England) Regulations 2013**

[**Chapter one – Introduction**](#Chapter1)

[**Chapter two – What are the powers?**](#Chapter2)

[**Chapter three – Who is authorised to use these powers?**](#Chapter3)

[**Chapter four – How should these powers be used?**](#Chapter4)

[**Chapter five – Safeguards**](#Chapter5)

**Important – please read:** 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.

1. **Introduction**

What is the purpose of this code of practice?

The code introduced powers for authorised local authority officers to obtain information from listed organisations about their customers, in order to combat fraud against East Devon District Council.

These powers form part of the Council Tax Reduction Schemes (Detection of Fraud and Enforcement) (England) Regulations 2013. These Regulations are made under sections 14A to 14C of the 1992 Act (inserted by section 14 of the 2012 Act) and make provision for powers to require information as well as the Prevention of Social Housing Fraud Act 2013 section 7.

Who is this code of practice for?

This code of practice is intended for

* East Devon District Council Officers who are authorised by the Chief Finance Officer (within the meaning of section 5 of the act), subject to paragraphs (2) and (3) under regulations 4 and 5 of The Council Tax Reduction Schemes (Detection of Fraud and Enforcement) (England) Regulations 2013 to obtain information form persons set out in Section 4 (3)
* persons from whom information may be required under these powers, and
* to members of the public who wish to know more about the powers.

Which organisations are required to provide information?

The organisations listed in the Act, for example banks, may hold information that could help to detect Council Tax offences. [A list of organisations is given in chapter two](#Provideinfo).

1. **What are the powers?**

Who is authorised to request information?

Only officers that have received authorisation may make requests for information under these powers. They will have received full training in the correct application of these powers. The numbers of authorised officers will be strictly limited. More information about authorised officers is contained in chapter three.

How should the powers be used?

In order to comply with provisions in the Human Rights Act 1998, these powers should be used as a last resort. Authorised officers will be able to use them only where it is necessary to do so. This means that they must consider whether there are other less intrusive means of obtaining the information.
Authorised officers will be able to request information in order to ensure that Council Tax offences can be detected and punished. For example a Building Society may have information about a customer’s savings account. If that customer is receiving Council Tax Support on the grounds of having no savings or capital then they may be committing fraud. Knowing about the account may help East Devon District Council put a stop to fraud. Under Section 4 of the Act, any organisation that fails to provide information when asked to do so under these powers may be prosecuted.

What are the safeguards against the misuse of the powers?

Authorised officers may obtain information only where they are allowed to by law, and they are obliged to maintain the security and confidentiality of all information that they may receive as a result of their duties. There are strict penalties for unauthorised requests for, or disclosure of, information. Comments or complaints about the use of these powers may be made to the Corporate Fraud and Compliance Team Leader.

Who can be required to provide information?

(2) The persons who fall within this paragraph are—

(a) any person who is or has been an employer or employee within the meaning of any provision made by or under the Contributions and Benefits Act;

(b) any person who is or has been a self-employed earner within the meaning of any such provision;

(c) any person who by virtue of any provision made by or under that Act falls, or has fallen, to be treated for the purposes of any such provision as a person within sub-paragraph (a) or (b);

(d) any person who is carrying on, or has carried on, any business involving the supply of goods for sale to the ultimate consumers by individuals not carrying on retail businesses from retail premises;

(e) any person who is carrying on, or has carried on, any business involving the supply of goods or services by the use of work done or services performed by persons other than employees of that person;

(f) any person who is carrying on, or has carried on, an agency or other business for the introduction or supply, to persons requiring them, of persons available to do work or to perform services;

(g) any local authority acting in their capacity as an authority responsible for the granting of any licence;

(h) any person who is or has been a trustee or manager of a personal or occupational pension scheme; or

(i) the servants and agents of any person as is specified in any of sub-paragraphs (a) to (h).

(3) The persons who fall within this paragraph are—

(a) any bank;

(b) the Director of Savings appointed under section 1(1) of the National Debt Act 1972([**7**](http://www.legislation.gov.uk/uksi/2013/501/made#f00007));

(c) 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;

(d) any insurer;

(e) 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;

(f) any water undertaker or sewerage undertaker;

(g) any person who—

(i) is the holder of a licence under section 7 of the Gas Act 1986([**8**](http://www.legislation.gov.uk/uksi/2013/501/made#f00008)) to convey gas through pipes; or

(ii) is the holder of a licence under section 7A(1) of that Act([**9**](http://www.legislation.gov.uk/uksi/2013/501/made#f00009)) to supply gas through pipes;

(h) any person who (within the meaning of the Electricity Act 1989([**10**](http://www.legislation.gov.uk/uksi/2013/501/made#f00010))) distributes or supplies electricity;

(i) any person conducting any educational establishment or institution;

(j) anybody the principal activity of which is to provide services in connection with admissions to educational establishments or institutions;

(k) the Student Loans Company; or

(l) any servant or agent of any person mentioned in sub-paragraphs (a) to (k).

What types of information will be requested?

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

* 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 finance company

When and about whom may authorised officers require information?

Authorised officers may only obtain information that relates to a particular person identified by name or description. In a minority of cases this may involve seeking to identify a suspected fraudster using his description (for example male, aged mid- thirties) and checking this against the address he uses. For example, in the case of an allegation that an individual is working and this has not been declared to East Devon District Council we would write to the employer and identify the individual by their National Insurance Number, among other things. We will do all we possibly can to eliminate any risk of our obtaining information about innocent third parties, which would be a breach of the Data Protection Act. Authorised officers would not be able to ask a company to provide details of all its employees. Enquiries must be reasonable in relation to the purposes set out in the legislation.

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

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

This means that authorised officers may make enquiries where they have reasonable grounds for believing that a person is committing fraud, helping someone else to do so, or being lied about as part of a Council Tax Support claim or housing application in respect of them.

For example:

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

Information may also be requested, for example, where it was suspected that a claimant had not disclosed capital held in a bank account. However, no information will be requested that is the subject of legal privilege - this is confidential communications between a legal adviser and his/her client for the purposes of giving or receiving legal advice, or any information obtained or documentation prepared for the purposes of legal proceedings. For example, authorised officers may not request confidential client information from a bank's solicitor. However, information such as financial details contained in a loan application that does not constitute confidential communication for the purposes of obtaining legal advice and information concerned with the furthering of a criminal offence, is not protected by legal privilege.

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

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

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

Authorised officers will not be able to make enquiries about family members who fall outside the definition given above. So, in the example, the authorised officer will not be able to make enquiries about a daughter who has left home and is working.

Who will we go to first for information?

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

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

of his business in the United Kingdom.

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

permission under paragraph 15 of that schedule (as a result of qualifying for authorisation under paragraph 12 of that Schedule) to effect or carry out contracts of insurance.

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

1. **Who is authorised to use these powers?**

Only those local authority officers that have been authorised by the Chief Executive or Chief Finance Officer may use these powers. These officers are known as authorised officers.

The numbers of staff eligible for authorisation will be limited to those who have received appropriate training.

Authorised officers will hold a certificate of their authority.

Authorised officers have no direct role in making decisions on entitlement to Council Tax Support or the granting of a tenancy.

How will officers be authorised?

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

How will officers be trained?

Authorised officers, must have received full training in the use of these powers. They must have completed appropriate training in investigative techniques, data protection and human rights legislation. This is contained in relevant parts of the Professionalism in Security (PINS) syllabus or its equivalent. Authorised officers will not be able to access on-line information until they have received suitable training.

**4. How should the powers be used?**

What will information providers need to know?

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

The Data Protection Act 1998 will not be contravened by providing the information requested by authorised officers. Under Section 35(1) of the Data Protection Act 1998 exemption from the non-disclosure provisions exists where a statutory provision, such as

Section 109B and C of the Administration Act, requires the supply of information.

What details should requests for information contain?

All requests for information will include the following details.

* the identity of the authorised officer who is making the request, and to whom the information should be sent;
* sufficient information to ensure that the customer, and the particular account in question, can be identified from the information provided. This may include such detail as a date of birth, address or customer reference number; and
* the address to which the information must be sent.

To whom should enquiries be addressed?

All enquiries will be made to the organisation involved. This is because it is organisations that are listed in the legislation (Section 109A(2A) of the Administration Act) on whom the requirement to provide information is placed. The enquiry must be addressed to the organisation, care of the most senior individual within that organization that the authorised officer can identify. If there were evidence of intentional failure to provide information it would be the organisation that faced prosecution and not the individual. Initially, refusals would be taken to the most senior level in an organisation in order to secure compliance with a request. In exceptional circumstances, it is possible that only an individual rather than the precise name of an organisation could be identified. Where this happened then the request would be made to the most senior

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

What happens when an organisation fails to provide information?

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

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

likely to be provided.

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

What are reasonable grounds?

Under no circumstances will authorised officers use these powers unless they think it is reasonable to do so. What is reasonable will vary, depending on the circumstances of the case, and each case should be considered on its own merits. The decision of the authorised officer will be judged against what another person acting in good faith and in the same situation as the authorised officer might consider to be reasonable. Examples of what an authorised officer would consider when deciding whether or not his/her use of these powers is reasonable include:

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

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

or validators.

For example:

* A claimant has declared savings of £2, 000 on his initial claim form. Some time later, an allegation is received that his savings are more substantial than this. In this instance, the investigator should question the claimant in the first instance, and he may be asked to provide copies of his bank or building society statements. If he refused, the investigator should ask for permission to contact his bank or building society directly. If he still refused, the investigator should ask an authorised officer to make an enquiry of the bank or building society under the terms of the Fraud Act.
* An investigator has obtained a statement from an employer which appears to confirm that a claimant is in full-time employment. The investigator asks an authorised officer to obtain detailed bank statements to confirm the employer's statement and possibly uncover other undisclosed income. There is no reason to suppose that the employer's statement is inaccurate. Neither does the investigator explain why he has reasonable grounds to suspect that there is any other undisclosed income. The authorised officer consequently rejects the request as the information is neither necessary nor are there reasonable grounds to suspect the existence of undisclosed income.

Management checks will ensure that these procedures are followed correctly. Any enquiry made without good reason could lead to disciplinary action against the officer concerned.

**How will information be requested?**

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

Authorised officers will not make enquiries in person by means of a visit. However, they may make arrangements to telephone the organisation if they need to discuss the information that has been provided. No new enquiries will be made in the course of this contact. Authorised officers will not issue requests by either fax or e-mail without prior agreement with the information provider. Information providers will be able to make replies in a way that has been agreed with the authorised officer. Authorised officers must take account of what would suit the organisation providing the information when deciding how information should be returned - for example, if the authorised officer makes a request by e-mail, it would not oblige the information provider to reply in the same manner.

Authorised officers will make enquiries of specific information providers only where they have reasonable grounds for believing that they hold information on a particular individual. For example, authorised officers will not normally issue requests to all UK

banks asking if they have information on a particular customer. However, such requests may be made in a small number of the most serious cases where the information cannot be obtained by other means. This would only be done in consultation with the local authority Benefits, Corporate Fraud & Compliance Team Leader.

How will authorised officers manage requests for information?

Local authorities must take all reasonable steps to keep to a minimum the number of officers authorised to use these powers and to centralise enquiries within the local authority. Local authorities should consider whether it would be possible to work with another local authority in order to reduce the number of sources from which organisations may receive requests for information.

Local authorities will manage requests in such a way as to cause the least inconvenience to the data provider. If, for example, a bank has nominated a central point of contact within its organisation for receiving enquiries, local authorities will be expected to direct their enquiries to it.

How will information be used?

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

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

Information sharing

Section 122 of the Administration Act and Section 110 of the Finance Act 1997 enable the DWP, the Inland Revenue and HM Customs and Excise to share information for the prevention and detection of fraud and to ensure the accuracy of the information

held by each Department. If information is received which suggests that taxes are being evaded, or that another crime is being committed, then DWP will pass on relevant information to other departments and local authorities.

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

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

The procedures and standards which are to be adhered to for the disclosure of information and for the prevention of unauthorised disclosure are already enshrined in law and in existing guidance to staff. These provisions ensure that those who obtain or disclose information unlawfully can be punished, thereby providing a deterrent against misuse.

**5. Safeguards**

Confidentiality and security

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

* information is only used for lawful purposes notified to the Information Commissioner;
* 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.

Records are kept of all access to electronic information using the powers in the Fraud Act. This means that management knows who has accessed the information, on whose behalf and for what reason. Management will undertake regular checks.

The fair collection of data

The first data protection principle requires that information obtained by the use of these powers be collected lawfully and fairly. The Fraud Act provides for the lawful processing of such information. Local authority claim forms and leaflets will inform customers that information may be sought about them from certain third parties.

The Information Commissioner

The Information Commissioner is responsible for the promotion of good practice regarding the processing of personal data. She may take action for a breach of the Data Protection Act 1998. Further information can be obtained from: The Office of the Information Commissioner, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Penalties for unlawful disclosure

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

a. the unauthorised disclosure of social security information (Section 123 of the Administration Act). An offence under this Act is punishable by imprisonment for up to two years and/or a fine;

b. unauthorised access to computers (Section 1 of the Computer Misuse Act 1990). An offence under this Act is punishable by imprisonment for up to six months and/or a fine; and

c. the unlawful obtaining or disclosure of personal data (Section 55 of the Data Protection Act 1998).

Retention and storage

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

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

Complaints

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

Local authorities are independent statutory bodies with responsibility for the administration of Housing Benefit and Council Tax Support. Each authority has its own mechanism for handling complaints about the way in which it operates. If the complaint

relates to the way that a local authority authorised officer has used the powers, reference should be made to the complaints procedure that each local authority has in place.

Serious complaints relating to local authority use of electronic access should be addressed to the Chief Executive of the local authority concerned.

The Local Government Ombudsmen

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

**England**

Local Government Ombudsman

21 Queen Anne's Gate

London SW1H 9BU

**Scotland**

Local Government Ombudsman

23 Walker Street

Edinburgh EH3 7HX

**Wales**

Local Government Ombudsman

Derwen House

Court Road

Bridgend CF31 1BN

Subject Access

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

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

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

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

Appeals against benefit decisions

Customers' normal rights of appeal are not affected by the use of powers to obtain information from the private and public sector. A customer has the right to dispute or appeal against a Council Tax Support decision, including a decision based on the results of an investigation into an inconsistency identified by the use of these powers. If the customer has disputed the decision but remains dissatisfied with the outcome, they can still appeal in the usual way.

If a customer is not satisfied with the way in which their case is managed, they should contact the local authority office. The complaint will be dealt with as quickly as possible.