

# **SURVEILLANCE UNDER THE REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA) AND THE INVESTIGATORY POWERS ACT 2016**

## **POLICY AND PROCEDURES**

**FEBRUARY 2020**

### **1.0 INTRODUCTION**

The Regulation of Investigatory Powers Act 2000 (RIPA) and the Investigatory Powers Act 2016 (IPA) provide a regulatory framework which enables public authorities to obtain information through the use of certain covert investigatory techniques. RIPA includes frameworks around the use of directed surveillance and the use of covert human intelligence sources (CHIS).

The Investigatory Powers Act 2016 (IPA) provides the framework in which communications data can be accessed and obtained. This policy summarises how Cheshire East Council is able to use these frameworks and how applications can be lawfully made. It also provides directions regarding the storage, use and retention of information and data obtained from the use of such actions.

The Protection of Freedoms Act 2012 requires that applications to use directed surveillance and covert human intelligence sources (CHIS) must have prior judicial approval and that the use of these techniques is limited to the investigation of offences which attract a minimal custodial sentence of 6 months.

The Investigatory Powers Act (2016) (IPA) outlines how enforcement agencies can access and obtain communications data, as well as specifying the types of data which can be obtained. Dependent on the type of data being requested, such a request is limited to the investigation of offences which attract a minimal custodial sentence of 6 months (entity data) or 12 months (event data).

The Investigatory Powers Commissioners Office (IPCO) has responsibility for oversight of all investigatory powers since the implementation of IPA 2016.

**OFFICIAL**

## **2.0 BACKGROUND**

An individual has rights, freedoms and expectations are guaranteed by the European Convention on Human Rights and the Human Rights Act 1998. Using the powers under RIPA and IPA can conflict with and cause the suspension of an individual's human rights. Therefore, when investigating wrongdoing, it is important that certain conditions are met in each case so that evidence is obtained lawfully, in order to support any enforcement action as deemed necessary in line with the Council's Enforcement Policy.

By following the authorisation procedures set out by RIPA and IPA, officers of the Council are ensuring that they can demonstrate that the surveillance is necessary for a purpose permitted by the Human Rights Act 1998 and that it is a proportionate measure to take. Compliance with RIPA and IPA will significantly reduce the likelihood of any surveillance carried out by the Council being unlawful, and therefore subject to legal challenge.

Cheshire East Council will occasionally need to use covert surveillance/CHIS/access communications data in order to carry out its enforcement functions effectively. Examples of such enforcement activities are planning enforcement, licensing enforcement, trading standards, environmental health and community protection investigations. Powers under RIPA/IPA can be used where it is demonstrated that viable alternatives to obtaining evidence to mount a prosecution have been considered, but are not appropriate and that any collateral intrusion has been considered.

## **3.0 USE OF COVERT SURVEILLANCE IN LOCAL AUTHORITIES**

Local authorities are not authorised to carry out any form of intrusive surveillance. Intrusive surveillance is defined in Section 26 (3) of RIPA as:

- covert surveillance, which is carried out in relation to anything taking place on any residential premises or in any private vehicle, and involves the presence of an individual on the premises or in the vehicle, or is
- carried out by means of a surveillance device (e.g. a listening or tracking device in a person's home or in his/her private vehicle).

Local authorities are restricted to use of the three techniques mentioned above, i.e.

- using 'directed' surveillance
- deploying a Covert Human Intelligence Source (CHIS)
- acquiring communications data.

The Council is required to obtain the authorisation of a Director listed in Schedule 1 of this policy before using directed surveillance. The use of a CHIS can only be authorised by the Chief Executive. Before acquiring communications data, the Council is required to have a 'made aware' officer within the application process. This is usually at Service Manager level (the

OFFICIAL

'made aware' officer does not have to be independent) as well as the Compliance and Customer relations team.

When using directed surveillance or deploying a CHIS, approval must also be granted by a JP/Magistrate. The independent authorisation for local authorities when accessing communications data is provided by the Office for Communications Data Authorisations (ODCA), which has delegated powers from the Judiciary Commissioner.

### **3.1 Directed Surveillance**

Directed surveillance' is essentially covert surveillance in places open to the public. It is defined as:

- covert
- likely to obtain private information
- carried out in a publicly accessible place (including the internet)
- pre-planned against a specific individual or group
- conducted otherwise than as an immediate response to events

It includes surveillance by person or device to:

- observe someone's movements
- eavesdrop on conversations
- photograph or film people or events
- track vehicles

The Protection of Freedoms Act 2012 introduced a crime threshold, whereby local authorities are only able to use this power when investigating offences which attract a custodial sentence of six months or more, or offences relating to the sale of alcohol or tobacco products to minors.

### **3.2 Covert Human Intelligence Source (CHIS)**

A covert human intelligence can be either an undercover officer or a member of the public acting as an informant. The CHIS is someone who:

- establishes and maintains a relationship for a covert purpose
- covertly uses the relationship to obtain information or to provide access to information from another person
- covertly discloses the information derived from the relationship to the Council

Where the CHIS is under 18, special risk assessments need to be carried out for each case.

Before authorisation, a trained handler (day to day responsibility for dealing with the source) and controller (general oversight of the use made of the source) must be identified.

### **3.3 Obtaining Communications Data**

OFFICIAL

The Council is limited to accessing only entity and event data (see 7.2) i.e. the 'who', 'when' and 'where' of a communication – not the actual content.

Local Authorities must liaise with the National Anti Fraud Network (NAFN) to acquire Communications Data, as supported by the Investigatory Powers Commissioner's Office (IPCO).

- 3.4** The relevant regimes under which to make an application are as follows:
- a) Directed surveillance – RIPA
  - b) Use of a Covert Human Intelligence Source (CHIS) - RIPA
  - c) Obtaining communications data - IPA
- 3.5** If it is anticipated that there is a likelihood of obtaining confidential information as part of a covert action, e.g. legally privileged or medical information, then this must be disclosed during the application process and only authorised by the Chief Executive or, in his or her absence, an Executive Director.

## **4.0 APPLYING THE RIPA/IPA PRINCIPLES AND CONCEPTS**

### **4.1 The tests of necessity and proportionality**

Use of covert techniques should only be authorised if the Authorising Officer/ODCA is satisfied that the action is both **NECESSARY** and **PROPORTIONATE**. The Human Rights Act 1998 defines a measure or action as proportionate if it:

- impairs as little as possible the rights and freedoms of the individual concerned and of innocent third parties, and
- is carefully designed to meet the objectives in question, is not arbitrary, unfair or based on irrational considerations.

### **4.2 Collateral intrusion**

The Authorising Officer/OCDA must also take into account the risk of intrusion into the privacy of persons other than those who are directly the subject of the investigation or operation. This is termed "collateral intrusion". Officers carrying out the covert action should inform the Authorising Officer/ODCA if the investigation or operation unexpectedly interferes with the privacy of individuals who are not covered by the authorisation. Consideration should be given to whether the authorisation should be amended and re-authorised or whether a new authorisation is required.

## **5.0 PROCEDURES FOR IMPLEMENTING COVERT ACTIVITY**

### **5.1 General**

All covert activity must be properly authorised and recorded, the tests of necessity and proportionality must be satisfied and the potential for collateral intrusion must be considered and minimised. The table below outlines the requirements for each activity:

OFFICIAL

Covert technique	Legislation and regime	Crime threshold	Approval
Directed surveillance	RIPA 2000	6 MONTHS (with exemptions)	Authorising Officer (Local Authority) and then Judicial
Covert Human Intelligence Source	RIPA 2000	6 MONTHS	Authorising Officer (Local Authority) and then Judicial
Obtaining Communications Data	IPA 2016	6 MONTHS – ENTITY DATA 12 MONTHS – EVENTS DATA (extra definition includes 'if it involves violence, results in substantial financial gain or by a large number of persons in pursuit of a common purpose')	'Made Aware' (Local Authority) Office for Communications Data Authorisations (ODCA) - NO more Designated Officer (Local Authority) and then Judicial

Any officer intending to undertake covert surveillance or use a covert human intelligence source must only do so if other means of obtaining information have been considered but are not viable.

Embarking upon covert surveillance or using a covert human intelligence source without authorisation, or conducting covert surveillance outside the scope of the authorisation, will mean not only that the “protective umbrella” of RIPA is unavailable, but it may result in disciplinary action being taken against the officer/officers involved. It may also result in the criminal investigation being compromised, as the evidence will be considered to have been obtained unlawfully. Unlawful acquisition (wilful or reckless) of communications data is a criminal offence.

Directed surveillance may only be carried out on residential premises if a member of the public has requested help or made a complaint to the Council, and if written permission to conduct the surveillance has been obtained from the resident from whose premises the surveillance will be carried out.

All relevant Council contracts issued to contractors/subcontractors must include a term that this policy and associated procedures are to be observed when operating on behalf of the Council.

## 5.2 Closed Circuit Television (CCTV)

CCTV systems are not normally within the scope of RIPA due to being overt. However, if they are used for a specific operation or investigation, or if automatic facial recognition by means of CCTV is used, RIPA authorisation for the use of directed surveillance by CCTV must be initially obtained by the investigating officer depending on who is leading the investigation.

OFFICIAL

Any covert activity utilising the CCTV system must comply with the Procedure Manual for the Operation of Cheshire East Council CCTV System.

### **5.3 Social Networking Sites (SNS) and other Internet sites**

The fact that a digital investigation is easy to conduct does not reduce the need for authorisation when necessary and consideration must be given to whether authorisation under RIPA should be obtained.

Different social network sites (SNS) work in different ways and could be considered “open source” if privacy settings are not applied. It is the responsibility of the individual account holder to apply privacy settings in order to protect against unsolicited access to their private information. There is a reasonable expectation of privacy if access controls are applied. Unprotected data may be deemed published and no longer under the control of the author.

Many officers would never envisage carrying out directed surveillance under RIPA; but, they may use SNS for a number of other reasons, such as HR monitoring is the activity of employees; or Children’s Services monitoring the SNS of parents; or chat rooms where they suspect children may be engaged in inappropriate activities. A single view is acceptable (best practice to record the viewing) - but repeat viewing may be considered to be monitoring and is therefore directed surveillance. Therefore may meet the criteria for authorisation as directed surveillance; or even a CHIS. Staff should make a record of any use of SNS or the internet which may assist in their enquiries and document the reasons for the search and the outcome. Officers should always consider other ways of obtaining the information required and document why those options have been discounted in favour of SNS.

If it is necessary and proportionate for the Council to covertly breach access controls, an authorisation for directed surveillance will be required. Consideration may need to be given to authorisation of a CHIS if the Council wishes to establish a relationship with an individual through a SNS or website, i.e. if the activity is more than mere reading of the site’s content.

An officer of the Council must not set up a false identity for covert purposes without authorisation.

An Online Investigations Policy has been developed to provide guidance to Cheshire East Council staff. Further guidance on this can be obtained from the Internal Audit Section or Trading Standards.

### **5.4 Officers able to make authorisations**

The authorisation of applications under the Regulation of Investigatory Powers (Directed Surveillance); or under the Covert Human Intelligence Sources Order 2010 (2010/521) can be authorised by a Director named in Schedule 1.

OFFICIAL

Under the IPA 2016 approval for access to and obtaining of communications data is granted only by the Office for Communications Data Authorisations (OCDA)

The Director of Governance and Compliance is not an Authorising Officer. This post assumes responsibility, as the Monitoring Officer, to ensure that the Council complies with the requirements of RIPA and IPA legislation.

Authorising Officers should not be responsible for authorising investigations or operations in which they have had or are likely to have any direct involvement. When such authorisation is required, this should be sought from an alternative Authorising Officer, as appropriate.

### **5.5 The role of the Investigating Officer**

It is the responsibility of the Investigating Officer to present the facts of the application, i.e.

- the crime to be investigated and the offence/sentence it attracts
- the reasons why it is proposed to conduct the investigation covertly
- what covert tactics are requested and why
- on whom the covert surveillance will be focused and who else may be affected by it
- how it is intended to conduct the surveillance
- the 'who, what, when, why and how'

### **5.6 The role of the Authorising Officer (CHIS and directed surveillance)**

It is the role of the Authorising Officer to:

- demonstrate to his/her satisfaction that use of covert surveillance is necessary for the crime being investigated by setting out in their own words why they are satisfied this is so
- demonstrate how he/she has reached the conclusion that the activity is proportionate to what it seeks to achieve and the reasons why the methods are not disproportionate
- ensure the application states explicitly what is being authorised and against which subjects, property or location. It is his/her responsibility to ensure those who conduct the surveillance are clear on what has been authorised.

The guidance below within point 5.6 has been offered within the CHIS Code of Practice (2018).

[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/742042/20180802\\_CHIS\\_code\\_.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742042/20180802_CHIS_code_.pdf)

In many cases involving human sources, a relationship will not have been established or maintained for a covert purpose. Many sources merely volunteer or provide information that they have observed or acquired other than through a relationship, without being induced, asked, or tasked by a public authority. This means that the source is not a CHIS for the purposes of the 2000 Act and no authorisation under the 2000 Act is required.<sup>7</sup>

OFFICIAL

## **Public volunteers**

**Example 1:** A member of the public volunteers a piece of information to a member of a public authority regarding something they have witnessed in their neighbourhood. The member of the public would not be regarded as a CHIS. They are not passing information as a result of a relationship which has been established or maintained for a covert purpose.

**Example 2:** A caller to a confidential hotline (such as Crimestoppers, the HMRC Fraud Hotline, the Anti-Terrorist Hotline, or the Security Service public telephone number) reveals that they know of criminal or terrorist activity. Even if the caller is involved in the activities on which they are reporting, the caller would not be considered a CHIS as the information is not being disclosed on the basis of a relationship which was established or maintained for that covert purpose. However, should the caller be asked to maintain their relationship with those involved and to continue to supply information (or it is otherwise envisaged that they will do so), an authorisation for the use or conduct of a CHIS may be appropriate.

## **Professional or statutory duty**

Certain individuals will be required to provide information to public authorities or designated bodies out of professional or statutory duty. For example, employees within organisations regulated by the money laundering provisions of the Proceeds of Crime Act 2002 are required to report suspicious transactions. Similarly, financial officials, accountants or company administrators may have a duty to provide information that they have obtained by virtue of their position to the Serious Fraud Office.

Any such regulatory or professional disclosures should not result in these individuals meeting the definition of a CHIS, as the business or professional relationships from which the information derives will not have been established or maintained for the covert purpose of disclosing such information.

Furthermore, this reporting is undertaken 'in accordance with the law' and therefore any interference with an individual's privacy (Article 8 rights) will be in accordance with Article 8(2) ECHR.

This statutory or professional duty, however, would not extend to the situation where a person is asked to provide information which they acquire as a result of an existing professional or business relationship with the subject but that person is under no obligation to pass it on. For example, a travel agent who is asked by the police to find out when a regular client next intends to fly to a particular destination is not under an obligation to pass this information on. In these circumstances, a CHIS authorisation may be appropriate.

## **Tasking not involving relationships**

OFFICIAL



Tasking a person to obtain information covertly may result in authorisation under Part II of the 2000 Act being appropriate. However, this will not be true in all circumstances. For example, where the tasking given to a person does not require that person to establish or maintain a relationship for the purpose of obtaining, providing access to or disclosing the information sought or where the information is already within the personal knowledge of the individual, that person will not be a CHIS.

**Example:** *A member of the public is asked by a member of a public authority to maintain a record of all vehicles arriving and leaving a specific location or to record the details of visitors to a neighbouring house. A relationship has not been established or maintained in order to gather the information and a CHIS authorisation is therefore not available. Other authorisations under the Act, for example, directed surveillance, may need to be considered where there is a possible interference with the Article 8 rights of an individual.*

### **Identifying when a human source becomes a CHIS**

Individuals or members of organisations (e.g. travel agents, housing associations and taxi companies) who, because of their work or role have access to personal information, may voluntarily provide information to public authorities on a repeated basis and need to be managed appropriately. Public authorities must keep such human sources under constant review to ensure that they are managed with an appropriate level of sensitivity and confidentiality, and to establish whether, at any given stage, they should be authorised as a CHIS.

Determining the status of an individual or organisation is a matter of judgement by the public authority. Public authorities should avoid inducing individuals to engage in the conduct of a CHIS either expressly or implicitly without obtaining a CHIS authorisation.

**Example:** *Mr Y volunteers information to a member of a public authority about a work colleague out of civic duty. Mr Y is not a CHIS at this stage as he has not established or maintained (or been asked to establish or maintain) a relationship with his colleague for the covert purpose of obtaining and disclosing information. However, Mr Y is subsequently contacted by the public authority and is asked if he would ascertain certain specific information about his colleague. At this point, it is likely that Mr Y's relationship with his colleague is being maintained and used for the covert purpose of providing that information. A CHIS authorisation would therefore be appropriate to authorise interference with the Article 8 right to respect for private or family life of Mr Y's work colleague.*

However, the tasking of a person should not be used as the sole benchmark in seeking a CHIS authorisation. It is the activity of the CHIS in exploiting a relationship for a covert purpose which is ultimately authorised by the 2000 Act, whether or not that CHIS is asked to do so by a public authority. It is possible, therefore, that a person will become engaged in the conduct of a

OFFICIAL

CHIS without a public authority inducing, asking or assisting the person to engage in that conduct. An authorisation should be considered, for example, where a public authority is aware that a third party is independently maintaining a relationship (i.e. “self-tasking”) in order to obtain evidence of criminal activity, and the public authority intends to make use of that material for its own investigative purposes.

#### **5.7 The role of JPs/Magistrate (CHIS and directed surveillance)**

The Protection of Freedoms Act 2012 amended the 2000 Act to make CHIS and directed surveillance authorisations by local authorities in England and Wales subject to judicial approval. These changes mean that local authorities need to obtain an order approving the grant or renewal of a CHIS authorisation from a Justice of the Peace before it can take effect. If the Justice of the Peace is satisfied that the statutory tests have been met and that the use of the technique is necessary and proportionate, they will issue an order approving the grant or renewal for the use of the CHIS as described in the application. The amendment means that local authorities are no longer able to orally authorise the use of CHIS.

#### **5.8 The role of the Office for Communications Data Authorisations (OCDA)**

The Office for Communications Data Authorisations considers requests for communications data from law enforcement and public authorities. OCDA carries out the important function of safeguarding an individual’s right to privacy under the Human Rights Act 1998. It makes independent decisions on whether to grant or refuse communications data requests, ensuring that all requests are lawful, necessary and proportionate.

#### **5.9 Outcomes**

The order which the Justice of the Peace/OCDA will complete, reflecting his/her decision, will identify one of the three following potential outcomes:

- Approval granted.
- Approval refused - the Council may not use the covert technique but may re-apply if significant new information comes to light or if technical errors in the initial application have been addressed.
- Refuse and Quash – the Council may not use the covert technique. This decision might be used where the JP/OCDA is of the opinion the application is fundamentally flawed.

#### **5.10 The role of the Director of Legal Services/Monitoring Officer**

The Director of Governance and Compliance (Monitoring Officer) is responsible for the integrity of the process as follows:

- ensuring compliance with all relevant legislation and with the Codes of Practice
- monitoring authorisations and conducting a quarterly review of applications, authorisations, refusals, reviews, renewals and cancellations.

OFFICIAL

### **5.11 The role of Elected Members**

It is considered good practice for Elected Members to undertake a formal scrutiny role in relation to RIPA/IPA and review the Council's use of it on an annual basis. However, they should not be involved in making decisions on specific authorisations.

The Monitoring Officer should ensure that an Annual Report regarding the Council's use of RIPA/IPA is submitted to the Council's Audit & Governance Committee.

## **6.0 PROCEDURES FOR GAINING APPROVAL (CHIS and Directed Surveillance)**

### **6.1 General**

At a departmental level, the application for authorisation must be in writing (electronically typed) and on the appropriate form, which must be completed in full. Officers should ensure that they use the current form available directly from the Home Office website.

Before applications are authorised they must be forwarded to the Compliance and Customer Relations Team to be checked and recorded in the Central Record of Authorisations. A unique reference number will be allocated at this stage. Officers requesting authorisation for directed surveillance and CHIS should complete a risk assessment, which should be submitted with the authorisation request.

### **6.2 Document Retention**

All relevant documentation, including a copy of the authorisation, a record of the period over which surveillance has taken place, any risk assessment, notebooks, surveillance logs and other ancillary documentation should be retained at departmental level for a period of six years from the date of cancellation of the surveillance, at which point they should be securely destroyed.

### **6.3 Duration of Authorisations**

Authorisation of directed surveillance will cease to have effect (unless renewed) either on specific cancellation (within the period of three months) or at the end of a period of three months (directed surveillance) or twelve months ("CHIS"), beginning with the day on which the authorisation was granted by the Justice of Peace/Magistrate.

Authorisation of communications data will cease to have effect when the requested authorised data is provided by the service provider.

### **6.4 Reviews**

Regular monthly reviews of authorisations should be undertaken by the Authorising Officer to assess the need for surveillance to continue. All reviews should be completed using the appropriate form. It is important to

OFFICIAL

note that reviews cannot broaden the scope of the original authorisation, but can reduce it for minor changes.

### **6.5 Renewals**

If, at any time before an authorisation would cease to have effect, the Authorising Officer considers it necessary for the authorisation to continue for the purpose for which it was given, he/she may renew it in writing. All applications for the Renewal of an Authorisation for Directed Surveillance should be on the appropriate form, which must be completed in full.

### **6.6 Cancellations and handling of surveillance material**

It is a statutory requirement that authorisations are cancelled as soon as they are no longer required. The Authorising Officer (or Investigating Officer in the first place) who granted (or last renewed) the authorisation must cancel it, if he is satisfied that the activity no longer meets the criteria for which it was authorised, or that it has fulfilled its objective.

If the Authorising Officer is no longer available, this duty will fall to the person who has taken over the role of the Authorising Officer. On cancellation of an authorisation, the Authorising Officer must be satisfied that the product of any surveillance is properly retained and stored or destroyed. If the surveillance product is of no evidential or intelligence value, it should be destroyed without delay, in accordance with Data Protection requirements. If the surveillance product is of potential evidential or intelligence value, it should be retained on the legal file, in accordance with established disclosure requirements, commensurate with any subsequent review.

When cancelling an authorisation, the Authorising Officer should:

- record date and times that surveillance took place and date the order to cease activity was made
- record reason for cancellation
- ensure surveillance equipment is removed and returned
- provide direction for management of product
- record value of surveillance, i.e. whether objectives of activity were met

### **6.7 Cessation of activity**

As soon as the decision is taken that the authorised activity should be discontinued, the instruction must be given to those involved to stop all surveillance of the subject, or to cease using the covert human intelligence source. Documentation detailing the date and time when any cancellation instruction was given by the Authorising Officer should be retained for a period of six years, at which point it should be securely destroyed.

### **6.8 Central Record of Authorisations**

The Compliance and Customer Relations Team is responsible for ensuring that a Central Record of Authorisations is maintained. This must be updated whenever an authorisation is granted, reviewed, renewed or cancelled. These

OFFICIAL

records should be securely retained for a period of three years from the ending of the authorisation, at which point they must be securely destroyed. It is necessary that the original hand signed (wet signature) authorisation is maintained within the Central Record of Authorisations, to provide a valid audit trail for court purposes. The Compliance and Customer Relations Team also retains copies of other RIPA forms such as those from the DWP where CEC staff are involved in surveillance but are not the lead officers. The Monitoring Officer should review and sign this Record on a quarterly basis.

With regard to directed surveillance, the Central Record of Authorisations will contain a copy of the authorisation, together with the following information:

- the type of authorisation
- the date the authorisation was given
- the name of the Authorising Officer
- the departmental reference number of the investigation or operation
- the title of the investigation or operation, including a brief description and names of subjects, if known
- date of approval from Magistrates Court, name of Magistrate and outcome
- whether the urgency or oral provisions were used, and if so why
- in the case of a self authorisation by the Authorising Officer, a statement in writing that he/she expressly authorised the action (only in exceptional circumstances)
- if the authorisation is renewed, the date of renewal and who authorised it, including the name and grade of the Authorising Officer
- whether the investigation or operation is likely to result in obtaining confidential information
- the date of cancellation of the authorisation
- where collateral intrusion may be an issue, a copy of the Privacy Impact Assessment

With regard to a CHIS, the Central Record of Authorisations must contain the following additional information:

- a copy of the authorisation, together with any supplementary documentation and notification of the approval given by the Authorising Officer
- a copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested
- the reason why the person renewing an authorisation considered it necessary to do so
- any urgent authorisation which was granted or renewed orally (in an urgent case) and the reason why the case was considered urgent
- the risk assessment made in relation to the source ("CHIS")
- a record of the results of any reviews of the authorisation
- the reasons, if any, for not renewing an authorisation
- the reasons for cancelling an authorisation - cancellations are to be completed on the appropriate form

OFFICIAL

- the date and time when any instruction was given by the Authorising Officer to cease using a “CHIS”
- where collateral intrusion may be an issue, a copy of the Privacy Impact Assessment

With regard to applications for Communications Data, a separate Central Record of Authorisations will be maintained which will contain:

- a copy of the authorisation together with the following information:
    - applicant’s name and job title
    - the operation name, including a brief description of the nature of the operation and names of subject(s) if known
- 6.9 Additional requirements for authorisation of covert human intelligence sources only
- 6.9.1 Covert human intelligence sources may only be authorised if the following additional arrangements are in place:
- There is an employee of the Council with day to day responsibility for dealing with the source and, for the source’s security and welfare, there is a Senior Officer who has general oversight of the use made of the source.
  - An officer who is responsible for maintaining a record of the use made of the source; these records will contain any matters specified by the Secretary of State – The Regulation of Investigatory Powers (Source Records) Regulations 2000 (SI 2000/2725) set out these matters.
  - Records disclosing the identity of the source and the information provided by him/her will not be made available to others except on a need to know basis
- 6.9.2 Vulnerable individuals (i.e. a person who is in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care or protect himself against significant harm or exploitation) may be authorised to act as a CHIS only in the most exceptional circumstances.
- 6.9.3 Authorisations for juvenile sources (under 18) should only be granted if the provisions contained in The Regulation of Investigatory Powers (Juveniles) Order 2000 (SI 2000/2793) are satisfied. Any authorisation should be granted by the Chief Executive or (in his/her absence) an Executive Director. The duration of an authorisation for the use or conduct of juvenile sources is four months.
- 6.9.4 If a juvenile source (under 18) is to be used, the Authorising Officer is responsible for obtaining the written consent of the parent or guardian or the person caring for the juvenile, unless to do so would compromise the juvenile’s welfare or safety. The Authorising Officer is also responsible for ensuring that an appropriate adult is present at any meeting. An appropriate adult is a parent or guardian, a person who has assumed responsibility for the wellbeing of the CHIS or, in their absence, a person who is responsible for the

OFFICIAL

wellbeing of the CHIS and who is over 18, who is neither a member of, nor employed by, the Council.

- 6.9.5 On no occasion should the use or conduct of a source under 16 years of age be authorised to give information against his/her parent or any person who has parental responsibility for him/her. The processing of information obtained as a result of surveillance should be restricted to specified employees. Only relevant senior managers should have access to the information collected to enable appropriate action to be taken. They must respect the confidentiality of all information and only disclose the information to other appropriate senior managers where further action is required.
- 6.9.6 When a CHIS is used, a “Handler” (who can be an Officer of the Council), and who must have received appropriate training, should be designated as having the day to day responsibility for dealing with the CHIS. This responsibility should also extend to the security, safety and welfare of the CHIS. In addition, a “Controller” should be designated to have the general oversight of the use made of the CHIS. These requirements also apply in cases in which the CHIS is an officer of the Council. The officer requesting authorisation for the use of a CHIS must also complete a risk assessment and submit it to the Authorising Officer, together with the authorisation request.
- 6.10 Test purchases of sales to juveniles  
When a young person (under 16 or under 18) carries out test purchases at a series of premises for age restricted products, it may be necessary to obtain an authorisation for ‘directed’ surveillance dependent on the product and relevant legislation; it is not necessary to prepare authorisations for each premises to be visited, providing each is identified at the outset but, in all cases, it is necessary to prepare a risk assessment in relation to the young person and to have an adult on hand to observe the test purchase.

## **7.0 AUTHORISATION FOR ACCESS TO COMMUNICATIONS DATA**

- 7.1 Local authorities are only able to access the who, what, where and when of communications data – not the content. The legislation requires that a Home Office accredited person, a Single Point of Contact (SPOC), facilitates the acquisition of the communications data requested. It is necessary for all local authorities to use the services of the National Anti-Fraud Network (NAFN) as SPOC to obtain communications data. This is compulsory and is supported by the Investigatory Powers Commissioner’s Office (IPCO).
- 7.2 The Office for Communications Data Authorisations (OCDA) was established to perform functions set out in the Investigatory Powers Act (IPA) 2016. The IPA builds on, and supersedes parts of, the Regulation of Investigatory Powers Act (RIPA) 2000.

OFFICIAL

The IPA has introduced a 'made aware' officer/rank within Local Authorities which should be the service manager as well as the Compliance and Customer Relations team. There are also offences for officers who obtain data unlawfully. The types of data which can be applied for now include entity and events data.

ENTITY DATA	EVENTS DATA
Subscriber detail Who is using device This data is about entities or links between them and describes or identifies the entity.	Calls or communications between devices (but not the content), known previously as traffic and service use. Numbers, texts Location data (known as cell site data)

## 8.0 APPLICATION PROCESS FOR ACCESS TO COMMUNICATIONS DATA

- Applicant completes online form on NAFN secure site (must be a registered user with NAFN).
- The application is sent electronically and the 'made aware' officer is notified. This is not an approval stage, just a review and confirmation the Local Authority is aware. The 'made aware' officer does not have to be independent.
- Once made aware, the application goes through to the NAFN SPOC with the possible outcomes being:
  - a) Rework requested
  - b) Reject - whole new application required
  - c) Authorise
- If authorised, the application is sent electronically to OCDA for review. It follows the same process as above. If it is rejected, seven days are allowed for it to be re-submitted.
- If it is approved, it is returned to the NAFN SPOC.
- The NAFN SPOC obtains data and information from service provider e.g. EE, O2, Vodafone.

### 8.1. When making an application, the following should be taken into account:

- Each application must stand alone.
- Acronyms and abbreviations must be avoided.
- The crime/purpose, legislation, offence and penalties must be clearly stated.
- Dates must be specific (e.g. intelligence).
- The objective of the application and how the data will be used must be clearly stated.
- Standard terms, e.g. suspect, witness, victim must be used.
- It is imperative to be specific about how attribution has been attempted, e.g. has the applicant called the number?

## 8.2 What Communications Data can Local Authorities request?

### Telephony

- Attribution – subscriber details (name and address of subscriber).
- If 'pay as you go' – top up history, customer notes.
- Call data.

OFFICIAL



- Location data – start location and end location of a call. Triangulation from mobile cell sites that can be mapped via longitude and latitude. Also with a cell mast location number it is possible to map its coverage via the provider.
- Mobile data event record – shows when data has been used (e.g. logging onto an app) but not the content.
- IMEI/SIM/IMSI – SIM linked to device, shows device capability and numbers linked including network usage.

#### **Internet**

- IP addresses – internet protocol address (IPV4 and IPV6) address for a device connecting to the internet – both static and dynamic. Static is usually home internet or often business - dynamic may be shared.
- Social Media and Apps – basic subscriber details, log on history – not the content.
- Email – registration details, log on history, email headers
- Websites – registrant details, preservation of pages, linked services
- Gaming platforms – account details classed as communications data.
- Skype and similar (e.g. Google Talk) – user name and IP address

#### **Others**

- Postal/Couriers are covered if there is more than one collection. The Council is able to obtain sorting, conveyance, distribution and delivery details.

### **9. INSPECTIONS**

The oversight for all investigatory powers is now consolidated under one commissioner – the Investigatory Powers Commissioners Office (ICPO). ICPO will carry out direct inspections with the Council for the use of directed surveillance and CHIS. In respect of communications data, the inspection will be made of NAFN, with a potential to request further information from the Council.

### **10.0 TRAINING**

Regular training sessions for Authorising Officers, 'Made Aware' and Investigating Officers will be arranged internally. No officer who has not attended a training session will be permitted to instigate or authorise any application for the use of RIPA/IPA powers.

OFFICIAL