APPENDIX A

East Herts District Council

Regulation of Investigatory Powers Act 2000

Policy

Document Control

Organisation	East Hertfordshire District Council
Title	Regulation of Investigatory Powers Act 2000 Policy
Author – name and title	James Ellis, Head of Legal & Democratic Services
Owner – name and title	James Ellis, Head of Legal & Democratic Services
Date	June 2020
Approvals	Executive
Version	1.0
Next Review Date	June 2021

East Herts Council

Regulation of Investigatory Powers Act 2000
Policy

Contents:

Page

1. Introduction

1.1. Summary

The Regulation of Investigatory Powers Act 2000 ("RIPA") came into force on 25 September 2000 and sought to regulate covert investigation practices undertaken by a number of bodies, including local authorities.

This Policy is the framework on which East Herts Council ("the Council") applies the provisions of RIPA as it relates to covert surveillance. It must be read in conjunction with the statutory codes of practice issued by the Secretary of State and any additional guidance provided by the Investigatory Powers Commissioner's Office (the "IPCO") (formerly the Office of Surveillance Commissioners – OSC) and individual Services to deal with the specific issues of their service.

1.2. Background

The Human Rights Act 1998 requires the Council to have respect for the private and family life of citizens. However in rare cases, it may be lawful, necessary and proportionate for the Council to act covertly in ways that may interfere with an individual's rights.

The rights conferred by Article 8 of the Human Rights Act are not absolute rights, but qualified right, meaning that it is still possible for a public authority to interfere with those rights provided the following criteria are satisfied;

(a) It is done in accordance with the law
(b) It is necessary (as defined in this document); and
(c) It is proportionate (as defined in this document).

RIPA provides a statutory mechanism for authorising certain types of surveillance. It seeks to ensure that any interference with an individual's right under Article 8 is necessary and proportionate. In doing so, RIPA seeks to ensure both the public interest and the human rights of individuals are suitably balanced.

It is possible that unauthorised surveillance will be a breach of a person's right to privacy under Article 8. Even if surveillance without due authorisation in a particular instance is not illegal, if authorisation is not

obtained, the surveillance carried out will not have the protection that RIPA affords.

If the correct procedures are not followed;

- evidence may be disallowed by the courts,
- a complaint of maladministration could be made to the Ombudsman, and/or
- the Council could be ordered to pay compensation

It is therefore essential that this document, along with any further guidance that may be issued from time to time by the Head of Legal and Democratic Services, always be complied with.

1.3. Policy Review

RIPA and this document are essential for the effective, efficient and legal operation of the Council's covert surveillance activity. This document will, therefore be kept under annual review by the Head of Legal and Democratic Services.

Authorising Officers, as defined below, must bring any suggestions for the continuous improvement of this document to the attention of the Head of Legal and Democratic Services, at the earliest possible opportunity.

1.4. Scope

RIPA does not;

- Make unlawful anything that is otherwise lawful
- Impose any new statutory duties, or
- Prejudice or disapply any existing powers available to the Council to obtain information by any means not involving conduct that is governed by RIPA. (For example it does not affect the Council's current powers to obtain information from the DVLA or the Land Registry).

If RIPA procedures are followed correctly the conduct of an investigation will be deemed lawful for all purposes (section 27 RIPA). This protection extends to criminal and civil proceedings, Employment Tribunal hearings and a complaint to either the Local Government Ombudsman or the

Investigatory Powers Tribunal. It therefore provides protection both for the Council and any officer who may have been involved in an investigation.

It should also be noted that the requirements of RIPA, and this policy, extends to external agencies working on behalf of the Council. Where such agencies are carrying out the Authority's statutory functions, the Authority remains liable for compliance with its duties. It is essential that all external agencies comply with the regulations, as they are contractually obliged to do so.

RIPA provides a means of authorising certain acts of covert surveillance for a variety of purposes. To fully understand the effects of RIPA, it is essential to understand the various types of activity that are covered, and those that are not permitted, and the purposes that will justify surveillance.

The provisions of RIPA that apply to Local Authorities provide a regulatory framework that permits;

- The use of Directed Surveillance
- The Use of Covert Human Intelligence Sources
- The Acquisition and Disclosure of Communications Data

2. Definition of Surveillance

"Surveillance" includes:

- Monitoring, observing, listening to persons, watching or following their movements, listening to their conversations or their other activities or communications;
- Recording anything monitored, observed or listened to in the course of surveillance; and
- Surveillance by, or with, the assistance of a surveillance device, which will include cameras, video, and listening or recording devices.

Surveillance can be either overt or covert.

2.1. Overt Surveillance

The overwhelming majority of surveillance undertaken by the Council will be done overtly, meaning there will be nothing secretive or hidden

about the way it is conducted. In many cases officers will be going about Council business openly (e.g. a routine inspection by an Environmental Health Officer) or will have notified the subject of the investigation that they are likely to be under surveillance (e.g. where a noisemaker is warned (preferably in writing) that noise will be recorded if it continues.)

Overt surveillance does not require any authorisation under RIPA. Neither does low-level surveillance consisting of general observations in the course of law enforcement (for example, an officer visiting a site to check whether a criminal offence had been committed). Repeated visits may amount to systematic surveillance however, and require authorisation: if in doubt, advice should be sought from the Head of Legal and Democratic Service or the Senior Responsible Officer

Use of body worn cameras should also be overt. Badges should be worn by officers stating body cameras are in use and it should be announced verbally that recording is taking place. In addition, cameras should only be switched on when recording is necessary e.g. when issuing parking tickets.

2.2. Covert Surveillance

Covert surveillance is any surveillance that is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place.

It should be noted that if the same outcome can be achieved by overt means then those means need to be fully explored in the first instance. Covert surveillance must only be undertaken when there is no less invasive way of achieving the outcome.

3. Directed and Intrusive Surveillance

3.1. Directed Surveillance

Directed surveillance is surveillance which is covert, but not intrusive, and undertaken:

a) for the purposes of a specific investigation or specific operation;
b) in such a manner as is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation); and

c) otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under RIPA to be sought for the carrying out of the surveillance.

3.2. Intrusive Surveillance

Currently, local authorities are **not** authorised to carry out intrusive surveillance.

Surveillance becomes intrusive if the covert surveillance:

a) is carried out by means of a surveillance device in relation to anything taking place on any residential premises or in any private vehicle; or
b) where a device placed outside consistently provides information of the same or equivalent quality and detail as might be expected if it were in the premises or vehicle, or
c) is carried out in places ordinarily used for legal consultation, at a time when they are being used for such consultations

Therefore directed surveillance turns into intrusive surveillance if it is carried out involving anything that occurs on residential premises or any private vehicle and involves the presence of someone on the premises or in the vehicle or is carried out by means of a surveillance device **OR** when directed surveillance is carried out in places ordinarily used for legal consultation, at a time when they are being used for such consultations.

Residential premises are any part of premises occupied for residential purposes or living accommodation, including hotel rooms or prison cells. However, it does not include common areas in blocks of flats and similar premises.

A private vehicle is a vehicle used primarily for private purposes by the owner or person entitled to use it.

Commercial premises and vehicles are therefore excluded from intrusive surveillance.

Only the police or other law enforcement agencies are permitted to employ intrusive surveillance. Likewise, the council has no statutory powers to interfere with private property.

4. Identifying directed surveillance

You should ask yourself the following questions:

4.1. Is the surveillance overt or covert?

Refer to paragraphs 2.1 and 2.2 above. If your activities are not hidden from the subjects of your investigation, you are not within the RIPA framework at all. If the proposed surveillance is covert in nature, then refer to paragraph 4.2 below.

4.2. Can the same outcome be achieved by overt means?

Does the surveillance have to be covert? If not, then you should proceed with overt surveillance, including the use of signs and other notification techniques so that the subject of the surveillance is aware it is taking place.

4.3. Is the surveillance for the purposes of a specific investigation or a specific operation?

Although, the provisions of the Act do not normally cover the use of overt CCTV surveillance systems, since members of the public are aware that such systems are in use, there may be occasions when public authorities use overt CCTV systems for the purposes of a specific investigation or operation. For example, if the CCTV cameras are targeting a particular known offender. In such cases, authorisation for directed surveillance may be necessary.

4.4. Is the surveillance likely to result in the obtaining of private information about a person?

Private information is defined in RIPA section 26 (10) as including any information relating to a person's private or family life.

The European Court of Human Rights has considered this definition and has found that private life is a broad term not susceptible to exhaustive definition. Aspects such as gender identification, name, sexual

orientation and sexual life are important elements of the personal sphere protected by Article 8.

The Article also protects a right to identity and personal development and includes an individual's private or personal relationship with others. It includes an individual's business and family relationships. Family life itself should be treated as extending beyond the formal relationships created by marriage.

4.5. Is the surveillance otherwise than by way of an immediate response to events or circumstances where it is not reasonably practicable to get authorisation?

Directed surveillance does not include covert surveillance carried out by way of an immediate response to events or circumstances which, by their very nature, could not have been foreseen. For example, an environmental crime officer would not require an authorisation to conceal themselves and observe a suspicious person which they came across in the course of a routine patrol.

However, if as a result of that immediate response, you undertake a specific investigation you will need authorisation.

5. Covert Human Intelligence Sources (CHIS)

A person is a covert human intelligence source ("CHIS") if;

a) he establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraph (b) or (c);
b) he covertly uses such a relationship to obtain information or to provide access to any information to another person; or
c) he covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

A purpose is covert, in relation to the establishment or maintenance of a personal or other relationship if, and only if, the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose.

A relationship is used covertly, and information obtained is disclosed covertly if, and only if, it is used or disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question.

A member of the public who volunteers information to the Council is not a covert human intelligence source.

Likewise, members of the public who report allegations of anti-social behaviour and are asked to keep a note of incidents will not normally be CHIS either as they are not usually required to establish or maintain a covert relationship.

It should be noted, however, that if the information provided is recorded as potentially useful or actionable, there is potential duty of care to the individual and the onus is on the public authority to manage human sources properly. Authorising Officers should be alive to the possibility of 'status drift'. Authorising Officers, when deciding whether to grant an authorisation, should take account of the difference between a volunteer of information already known to the individual and the relevance of the exploitation of a relationship for a covert purpose.

5.1. Conduct and use

The conduct or use of CHIS must be authorised in accordance with RIPA.

Conduct of a CHIS. This is establishing or maintaining a personal or other relationship with a person for the covert purpose of (or is incidental to) obtaining or passing on information.

Use of a CHIS. This includes inducing, asking or assisting a person to engage in the conduct of a source, or to obtain information by means of the conduct of such a source.

The use of a juvenile CHIS may only be authorised for one month at a time.

5.2. Test Purchases

Carrying out test purchases will not require the purchaser to establish a relationship with the supplier with the covert purpose of obtaining information and, therefore, the purchaser will not normally be a CHIS.

For example, authorisation would not normally be required for test purchases carried out in the ordinary course of business (e.g. walking into a shop and purchasing a product over the counter).

By contrast, developing a relationship with a person in the shop, to obtain information about the seller's suppliers of an illegal product will require authorisation as a CHIS. Similarly, using mobile hidden recording devices or CCTV cameras to record what is going on in the shop, or an adult is observing a juvenile test purchase, this will require authorisation, as directed surveillance. In all cases, a prior risk assessment is essential in relation to any young person used for a test purchase.

5.3. Security and Welfare

Only the Chief Executive is able to authorise the use of vulnerable individuals and juvenile CHIS's. The Authorising Officer shall have regard to the special safeguards and provisions that apply to vulnerable individuals and juvenile sources, more particularly set out in the Covert Human Intelligence Source Code of Practice which can be found here.

The Authorising Officer shall ensure that arrangements are in place for the proper oversight and management of sources, including appointing individual officers for each source. The person responsible for the day-to-day contact between the public authority and the source will usually be of a rank or position below that of the Authorising Officer.

Officers using a source shall consider the safety and welfare of that source (even after cancellation of the authorisation), and the foreseeable consequences to others of the tasks they are asked to carry out. The Authorising Officer shall carry out a risk assessment before authorising the source.

6. Communications Data

The powers contained in Part 1 of Chapter 2 of RIPA permit Local Authorities to obtain information relating to the use of a postal service or telecommunications system for obtaining communications data and the disclosure to any person of such data. For these purposes, communications data includes information relating to the use of a postal service or telecommunications system but does not include the contents of the communication itself, content of e-mails or interaction with websites.

Communications data includes subscribers details, names and addresses and telephone numbers of those contacted, billing addresses, account information, web addresses visited etc.

Two types of data (Customer Data or Service Data) are available to local authorities and, when making an application for obtaining or disclosing such data, the applicant must specify exactly which type of information

A third type of data (Traffic data) is not accessible to local authorities.

6.1. Customer data – (Subscriber data, RIPA s21(4))

Customer data is the most basic. It is data about users of communication services. This data includes:

- Name of subscriber
- Addresses for billing, delivery, installation
- Contact telephone number(s)
- Abstract personal records provided by the subscriber (e.g. demographic information)
- Subscribers' account information – bill payment arrangements, including bank, credit/debit card details
- Other services the customer subscribes to.

6.2. Service data – (Service Use data, RIPA s21(4)(b))

This relates to the use of the service provider's services by the customer, and includes:

- The periods during which the customer used the service(s)
- Information about the provision and use of forwarding and re-direction services by postal and telecommunications service providers
- 'Activity', including itemised records of telephone calls (numbers called), internet connections, dates and times/duration of calls, text messages sent
- Information about the connection, disconnection and reconnection of services
- Information about the provision of conference calling, call messaging, call waiting and call barring telecommunications services

- Records of postal items, such as records of registered, recorded or special delivery postal items, records of parcel consignment, delivery and collection
- 'Top-up' details for prepay mobile phones – credit/debit card, voucher/e- top up details

6.3. Traffic data – (Traffic data, RIPA s21(6))

In relation to communications means:

- any data identifying or purporting to identify, any person, apparatus or location to or from which the communication is or may be transmitted
- any data identifying or selecting or purporting to identify or select apparatus through which, or by means of which the communication is or may be transmitted
- any data comprising signals for the actuation of apparatus used for the purposes of a telecommunications system for effecting (in whole or in part) the transmission of any communication and
- any data identifying the data or other data as data comprised in or attached to a particular communication but that expression includes data identifying a computer file or computer program access to which is obtained, or which is run by means of the communication to the extent only that the file or program is identified by reference to the apparatus in which it is stored.

7. RIPA Authorisation Procedure

7.1. General

Directed surveillance, the use of CHIS and the acquisition of communications data must be lawfully carried out in strict accordance with the terms of the relevant authorisation and Magistrates Court approval.

The Council can only authorise directed surveillance to prevent and detect conduct which constitutes one or more criminal offences. The criminal offences must be punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months imprisonment or be an offence under:

a) S146 of the Licensing Act 2003 (sale of alcohol to children);

b) S147 of the Licensing Act 2003 (allowing the sale of alcohol to children);
c) S147A of the Licensing Act 2003 (persistently selling alcohol to children); and
d) S7 of the Children and Young Persons Act 1933 (sale of tobacco etc. to persons under the age of 18)

The Council will only very rarely make use of CHIS so the applicant officer should consult the Head of Legal and Democratic Services before making an application for a CHIS authorisation in order to ensure that the current statutory requirements and best practice are being observed.

Applications for authorisations and notices requesting communications data must be processed through the Council's Home Office accredited single point of contact ("SPoC"). As the need to obtain such information will only very occasionally arise the applicant officer should contact the Head of Legal and Democratic Services before making an application in order to ensure that current statutory requirements and best practice are being observed.

All applications for authorisation must be sought and granted before any surveillance activity takes place. The decision whether or not to authorise an application must not be taken with the benefit of hindsight. This should be borne in mind when submitting an application to the Magistrates' Court.

Once approved, the original authorisation and accompanying paperwork must be forwarded to the RIPA Co-Ordinator (Senior Solicitor – Corporate Legal Team) to allocate the application a Unique Reference Number (URN) and for key details to be entered onto the central register.

7.2. Before Making the Application

Before making an application for an authorisation, the requesting officer must;

- read this policy document,
- determine whether the activity that they are proposing to conduct involves directed surveillance or the use of a CHIS,
- assess whether the activity will be in accordance with the law – is it governed by RIPA,
- assess whether the activity is necessary and why,

- assess whether the activity is proportionate.

If the activity can be conducted overtly or if a less intrusive option is available and practical, then that option should be pursued rather than obtaining a RIPA authorisation.

7.3. Special consideration in respect of confidential information

Particular attention is drawn to areas where the subject of surveillance may reasonably expect a high degree of privacy e.g. where confidential information is involved.

Confidential information consists of personal information (such as medical records or spiritual counselling), confidential journalistic material, confidential discussions between Members of Parliament and their constituents, or matters subject to legal privilege.

Legal privilege

Generally, this applies to communications between an individual and his/her legal adviser in connection with the giving of legal advice in connection with or in contemplation of legal proceedings. Such information is unlikely ever to be admissible as evidence in criminal proceedings.

If in doubt, the advice of the Head of Legal and Democratic Services should be sought in respect of any issues in this area.

Confidential personal information

This is oral or written information held in (express or implied) confidence, relating to the physical or mental health or spiritual counselling concerning an individual (alive or dead) who can be identified from it. Specific examples provided in the codes of practice are consultations between a health professional and a patient, discussions between a minister of religion and an individual relating to the latter's spiritual welfare or matters of medical or journalistic confidentiality.

Confidential journalistic material

This is material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence.

It should be noted that matters considered to be confidential under RIPA may not necessarily be properly regarded as confidential under section 41 Freedom of Information Act 2000.

Where such information is likely to be acquired, the surveillance may only be authorised by the Chief Executive or, in his absence, the person acting as the Head of Paid Service.

7.4. Who can give Provisional Authorisations?

Authorisations may only be given by the Authorising Officers listed in Appendix B. Only the Chief Executive can authorise the use of a CHIS, or the acquisition of confidential information (see paragraph 7.3 above).

Applications for the acquisition of Communications data can only be issued by a Home Office accredited single point of contact ("SPoC") (see paragraph 7.8 below)

It will be the responsibility of Authorising Officers who have been duly certified to ensure their relevant members of staff are also suitably trained as 'applicants' so as to avoid common mistakes appearing on forms for RIPA authorisations.

Training will be given, or approved by the Head of Legal and Democratic Services before Authorising Officers are certified to sign any RIPA forms. A central register of all those individuals who have undergone training or a one-to-one meeting with the Head of Legal and Democratic Services, on such matters, will be kept by the Head of Legal and Democratic Services.

Authorising officers should not normally be responsible for authorising operations in which they are directly involved, although it is recognised that this may sometimes be unavoidable. Where an Authorising Officer authorises such an investigation or operation the central register will highlight this and the Commissioner or inspector will be notified of this during his or her next inspection

Authorising Officers will also ensure that staff who report to them follow this guidance document and do not undertake or carry out any form of surveillance without first obtaining the relevant authorisations in compliance with this document.

Authorising Officers must also ensure that, when sending copies of authorisations and associated documentation to the Head of Legal and Democratic Services, that these are sent in sealed envelopes and marked 'Strictly Private and Confidential'.

Any equipment to be used in any approved surveillance must be properly controlled, recorded and maintained for audit purposes.

7.5. Grounds for Authorisation

An Authorising Officer has a number of obligations within the provisions of the Act, which must be met before carrying out any form of surveillance.

An Authorising Officer shall not grant a provisional authorisation for the carrying out of directed surveillance or for the use of a CHIS or for the obtaining or disclosing of communications data unless they have given **personal consideration** to the facts and believes:

a) that a provisional authorisation is <u>necessary</u>, and
b) the provisionally authorised investigation is <u>proportionate</u> to what is sought to be achieved by carrying it out

For local authority investigations, provisional authorisation is deemed "**necessary**" in the circumstances of the particular case if it is for the purpose of preventing and detecting crime or of preventing disorder.

Authorisation cannot be sought, and authority must not be given unless you are satisfied that the surveillance is "**proportionate**." You have to make sure that any interference with privacy is justified by the end being sought. Unless the benefit to be obtained from surveillance is significant, and unless the problem you are seeking to tackle is serious, the use of surveillance is unlikely to be proportionate.

The conduct must also be the least invasive method of achieving the end and the risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation must be assessed and taken into account (see Collateral Intrusion below).

Consideration must be given to the seriousness of the offence under consideration. Authorisation for directed surveillance can only be

granted if the purpose of the surveillance is the prevention or detection of crime(s) punishable by 6 months imprisonment or more, or relates to the sale or alcohol or tobacco to underage persons. Covert surveillance relating to dog fouling and other minor offences will not be deemed a proportionate activity.

Careful consideration needs to be made by authorising officers of all of these points. Such consideration needs to be demonstrated on the authorisation form in the relevant parts. Authorising Officers must exercise their minds every time they are asked to sign a form. They must never sign or rubber stamp the form without thinking about their personal and the Council's responsibilities.

Any boxes not needed on the form/s must be clearly marked as being 'not applicable' or a line put through the same. Great care must also be taken to ensure accurate information is used and inserted in the correct boxes. Reasons for any refusal of an application must also be kept on the form and retained for future audits.

7.6. Collateral Intrusion

Before provisionally authorising an investigation, the Authorising Officer shall also take into account the risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation; known as collateral intrusion. The investigating officer shall take measures, wherever practicable, to avoid or minimise unnecessary intrusion into the lives of those not directly connected with the investigation or operation.

An application for a provisional authorisation shall include an assessment of the risk of any collateral intrusion. The Authorising Officer shall take this into account, when considering the proportionality of the surveillance.

Where an operation unexpectedly interferes with the privacy of individuals who were not the subject of surveillance or covered by the authorisation in some other way, the investigating officer should inform the Authorising Officer.

7.7. Judicial Approval

The Council is only able to grant a provisional authorisation or renewal to conduct covert surveillance. No provisional authorisations, nor any surveillance granted under them, will take effect until judicial approval has been sought and granted by a Magistrates' Court.

Once the authorising officer has authorised the directed surveillance or CHIS, the investigating officer who completed the application form should contact the Magistrates' Court to arrange a hearing for the authorisation to be approved by a Justice of the Peace.

The investigating officer will provide the Justice of the Peace with a copy of the original authorisation and the supporting documents setting out the case. This forms the basis of the application to the Justice of the Peace and should contain all information that is relied upon.

In addition the investigating officer will provide the Justice of the Peace with a partially completed judicial application/order form.

The hearing will be in private and the investigating officer will be sworn in and present evidence as required by the Justice of the Peace. Any such evidence should be limited to the information in the authorisation.

The Justice of the Peace will consider whether he/she is satisfied that at the time the authorisation was granted or renewed, there were reasonable grounds for believing that the authorisation was necessary and proportionate.

The Justice of the Peace will also consider whether there continues to be reasonable grounds.

The Justice of the Peace must also be satisfied that the person who granted the authorisation was an appropriate designated person and the authorisation was made in accordance with any applicable legal restrictions, for example, the crime threshold for directed surveillance has been met.

The Justice of the Peace will record his/her decision on the order section of the judicial application/order form.
A copy of the RIPA form and judicial application/order form will be retained by the Court.

If the authorisation is approved the council may commence the activity.

If the Justice of the Peace refuses to approve the authorisation the council may not commence the activity although, if the reason for refusal is a technical error, the council may address this and reapply without going through the internal authorisation process again.

The Justice of the Peace may refuse to approve the authorisation, and quash it. The exercise of this power should not take place until the applicant has at least two business days from the date of the refusal to make representations.

7.8. Provisional Authorisation for Communication Data

The Act provides two different ways of provisionally authorising access to communications data; through a provisional authorisation under Section 22(3) and by a provisional notice under Section 22(4).

A provisional authorisation would, following judicial approval, allow the authority to collect or retrieve the data itself. A provisional notice is given to a postal or telecommunications operator and requires that operator to collect or retrieve the data and provide it to the authority serving the notice. An Authorising Officer decides whether or not a provisional authorisation should be granted or a provisional notice given.

A provisional authorisation under Section 22(3) may be appropriate where:

- the postal or telecommunications operator is not capable of collecting or retrieving the communications data;
- it is believed the investigation may be prejudiced if the postal or telecommunications operator is asked to collect the data itself;
- there is a prior agreement in place between the authority and the postal or telecommunications operator as to the appropriate mechanisms for the disclosure of data.

Notices and, where appropriate, provisional authorisations for communications data must be channelled through SPoC's. The SPoC is able to advise authorising officers as to whether an authorisation or notice is appropriate.

The Council use the services of the National Anti-Fraud Network (NAFN) for all Communications Data enquiries and as such NAFN performs the

role of a SPoC through their qualified SPoC officers. All applicants must be registered with NAFN via the NAFN website at www.nafn.gov.uk

Applications to obtain communications data should be made on the NAFN standard form available on the NAFN website and submitted in the first instance to the SPoC. If appropriate the SPoC will forward the application to a Council Authorising Officer for either the provisional authorisation of conduct or the provisional issuing of a notice.

If satisfied that the proposed investigation is both necessary and proportionate, the Authorising Officer will return the provisional authorisation or notice to the SPoC who will then liaise with the applicant and the postal/telecommunications company, after the appropriate Judicial Approval has been obtained. The disclosure of data under a notice will only be made to the Authorising Officer.

Communications data, and all copies, extracts and summaries of it must be handled and stored securely. The requirements of the Data Protection Act 2018 and the principles of the Criminal Procedure and Investigations Act 1996 must be strictly followed.

8. Activities by other public authorities

The investigating officer shall make enquiries of other public authorities e.g. the police whether they are carrying out similar activities if he considers that there is such a possibility in order to ensure that there is no conflict between the activities of this Council and those other public authorities.

9. Joint Investigations

When some other agency has been instructed on behalf of the Council to undertake any action under RIPA, this document and the forms in it must be used (as per normal procedure) and the agency advised or kept informed, as necessary, of the various requirements. They must be made aware explicitly what they are authorised to do.

When some other agency (e.g. police, Customs & Excise, Inland Revenue etc.):

a) wishes to use the Council's resources (e.g. CCTV), that agency must use its own RIPA procedures and, before any officer agrees to allow the Council's resources to be used for the other agency's purposes, they must obtain a copy of that agency's RIPA form for the record and/or

relevant extracts from the same which are sufficient for the purposes of protecting the Council and the use of its resources

b) wishes to use the Council's premises for their own RIPA action, the officer should, normally, co-operate with the same, unless there are security or other good operational or managerial reasons as to why the Council's premises should not be used for the agency's activities. In such cases, the Council's own RIPA forms should not be used as the Council is only assisting and not being involved in the RIPA activity of the external agency being involved in the RIPA activity of the external agency.

In terms of (a), if the police or other agency wish to use the Council's resources for general surveillance, as opposed to specific RIPA authorisations, an appropriate letter requesting the proposed use, remit, duration, details of who will be undertaking the general surveillance and the purpose of it must be obtained from the police or other agency before any Council resources are made available for the proposed use.

10. Duration, reviews, renewals and cancellation of authorisations

10.1. Duration

Authorisations must be reviewed in the time stated and cancelled once no longer needed.

Authorisations last for:

a) 12 months from the date of the judicial approval for the conduct or use of a source
b) three months from the date of judicial approval for directed surveillance
c) one month from the date of judicial approval for communications data, or earlier if cancelled under Section 23(8) of the Act.

However, whether the surveillance is carried out/conducted or not in the relevant period, does not mean that the authorisation is spent. Authorisations do not expire, they have to be reviewed, or cancelled if no longer required.

10.2. Reviews

The Authorising Officer shall undertake regular reviews of authorisations to assess the need for the surveillance to continue. The results of a review should be recorded on the central record of authorisations.

Where the surveillance provides access to confidential information or involves collateral intrusion the officer should conduct frequent reviews.

10.3. Renewals

If at any time before an authorisation ceases to have effect, it is necessary for the authorisation to continue for the purpose for which it was given, it may be renewed in writing for a further period of 3 calendar months, beginning with the day when the original authorisation would have expired. Magistrates Court approval is required before a renewal takes effect.

Authorisations may be renewed more than once, provided they continue to meet the criteria for authorisation and are approved by the Magistrates' Court. The renewal should be kept/recorded as part of the central record of authorisations.

The Authorising Officer must consider the matter afresh, including taking into account the benefits of the surveillance to date and any collateral intrusion that has occurred.

Authorisations can be renewed in writing shortly before the maximum period has expired. The renewal will begin on the day when the authorisation would have expired, provided the necessary judicial approval has been obtained.

An authorisation cannot be renewed after it has expired.

A further requirement in relation to renewal of a CHIS is that judicial approval will only be granted if the Magistrates are satisfied that a review has been carried out, which considers:

- the use made of the source in the period since authorisation was granted (or the last renewal); and
- the tasks given to the source during that period, and the information obtained from the conduct or use of the source

For the purposes of making an Order, the Magistrates have considered the results of that review.

10.4. Cancellations

The Authorising Officer must cancel an authorisation if they become satisfied that the surveillance is no longer required or appropriate.

Authorisations should not be allowed simply to lapse. The duty to cancel a notice falls on the Authorising Officer who issued it.

The Authorising Officer must then cancel the Application without delay. When cancelling the authorisation the Authorising Officer is required to consider whether the surveillance was effective, necessary and met its objectives. Cancellations must be made using the cancellation form and should briefly detail what product(s) resulted from the surveillance.

When cancelling an authorisation, the Authorising Officer must ascertain what recorded material has been obtained by the use of directed surveillance. The Authorising Officer should comment on the recorded material and how it is to be managed or used thereafter. If the matter is not proceeding to a prosecution, the Authorising Officer must be satisfied that any recorded material has been securely destroyed.

In the case of a notice issued in respect of communications data, the relevant postal or telecommunications operator will be informed of the cancellation.

11. Record Management

11.1. Central record of all Authorisations

The Head of Legal and Democratic Services shall hold and monitor a centrally retrievable record of all provisional and judicially approved authorisations. The Authorising Officer must notify and forward a copy of any provisional notice or authorisation granted, renewed or cancelled and any judicial approval received or refused within 1 week of the event to the Head of Legal and Democratic Services to ensure that the records are regularly updated.

The record will be made available to the relevant Commissioner or an Inspector from the Investigatory Powers Commissioner's Office. These

records will be retained for a period of 5 years from the ending of the authorisation. A record will be kept of the dates on which the authorisation notice is started and cancelled.

The Head of Legal and Democratic Services will monitor the submission of provisional and judicially approved authorisations and notices and give appropriate guidance, from time to time, or amend any provisional or draft document as necessary. The records submitted to the Head of Legal and Democratic Services, shall contain the following information:

a) the type of authorisation or notice
b) the date the provisional authorisation or notice was given;
c) name and rank/grade of the authorising officer;
d) the date judicial approval was received or refused;
e) the unique reference number (URN) of the investigation or operation;
f) the title of the investigation or operation, including a brief description and names of subjects, if known;
g) if the authorisation or notice is renewed, when it was renewed and who authorised the renewal, including the name and rank/grade of the authorising officer and the date of judicial approval;
h) whether the investigation or operation is likely to result in obtaining confidential information;
i) the date the authorisation or notice was cancelled.

11.2. Records maintained in the Department

The Authorising Officer shall maintain the following documentation, which need not form part of the centrally retrievable record:

a) a copy of the application and provisional authorisation or notice together with a copy of any order of judicial approval or refusal, as well as any supplementary documentation and notification of the approval given by the Authorising Officer;
b) a record of the period over which the surveillance has taken place;
c) the frequency of reviews prescribed by the Authorising Officer;
d) a record of the result of each review of the authorisation or notice;
e) a copy of any renewal of an authorisation or notice, together with judicial approval or refusal and the supporting documentation submitted when the renewal was requested;

f) the date and time when any instruction was given by the Authorising Officer,
g) the unique reference number for the authorisation (URN)

Each form must have a URN. The Authorising Officers will issue the relevant URN to applicants. The cross-referencing of each URN takes place within the form for audit purposes. Rejected forms will also have URN's.

11.3. Records relating to a CHIS

Proper records must be kept of the authorisation and use of a CHIS. An Authorising Officer must not grant a provisional authorisation for the use or conduct of a CHIS unless he believes that there are arrangements in place for ensuring that there is at all times a person with the responsibility for maintaining a record of the use made of the CHIS.

The records shall contain the following information:

a) the identity of the source;
b) the identity, where known, used by the source;
c) any relevant investigating authority other than the Council;
d) the means by which the source is referred to within each relevant investigating authority;
e) any other significant information connected with the security and welfare of the source;
f) any confirmation made by a person granting or renewing an authorisation for the conduct or use of a source that the information in paragraph (d) has been considered and that any identified risks to the security and welfare of the source have where appropriate been properly explained to and understood by the source;
g) the date when, and the circumstances in which, the source was recruited;
h) the identities of the persons who, in relation to the source;
    i. hold day-to-day responsibility for dealing with the source and for the source's security and welfare
    ii. have a general oversight of the use made of the source (not to be the person identified in h) i.
    iii. have responsibility for maintaining a record of the use made of the source

i) the periods during which those persons have discharged those responsibilities;
j) the tasks given to the source and the demands made of him in relation to his activities as a source;
k) all contacts or communications between the source and a person acting on behalf of any relevant investigating authority;
l) the information obtained by the conduct or use of the source;
m) any dissemination of information obtained in that way; and
n) in the case of a source who is not an undercover operative, every payment, benefit or reward and every offer of a payment, benefit or reward that is made or provided by or on behalf of any relevant investigating authority in respect of the source's activities for the benefit of that or any other relevant investigating authority.

Records which reveal the name(s) of the CHIS should only be disclosed to persons to the extent that there is a need for access to them; if legally necessary; or if ordered by any Court.

12. Retention and destruction

Generally, all material (in whatever media) produced or obtained during the course of investigations subject to RIPA authorisation should be processed, stored and destroyed in accordance with the requirements of the Data Protection Act 2018, General Data Protection Regulation (GDPR) (EU) 2016/679, the Freedom of Information Act 2000 and any other legal requirements, including those of confidentiality and the Council's policies and procedures regarding document retention.

Material obtained from properly authorised surveillance or a CHIS may be used in other investigations. Arrangements shall be in place for the handling, storage and destruction of material obtained through the use of covert surveillance, a CHIS or the obtaining or disclosure of communications data.

Authorising Officers must ensure compliance with the appropriate data protection requirements and any relevant Corporate Procedures relating to the handling and storage of material.

13. Social Media Sites

Whilst it is the responsibility of an individual to set privacy settings to protect unsolicited access to private information, and even though data may be

deemed published and no longer under the control of the author, it is unwise to regard it as "open source" or publicly available; the author has a reasonable expectation of privacy if access controls are applied. In some cases data may be deemed private communication still in transmission (instant messages for example).

Where privacy settings are available but not applied the data may be considered open source and an authorisation is not usually required. Repeat viewing of 'open source' sites, however, may constitute directed surveillance on a case by case basis and this should be borne in mind e.g. if someone is being monitored through their Facebook profile for a period of time and a record of the information is kept for later analysis, this is likely to require a RIPA authorisation for directed surveillance.

To avoid the potential for inadvertent or inappropriate use of social network sites in investigative and enforcement roles, Council Officers should be mindful of any relevant guidance and the Council's separate policy regarding the use of **Social Networking Sites and Conduct of Investigations**.

The Home Office Revised Code of Practice on Covert Surveillance and Property Interference, published in August 2018, provides the following guidance in relation to online covert activity:

'The growth of the internet, and the extent of the information that is now available online, presents new opportunities for public authorities to view or gather information which may assist them in preventing or detecting crime or carrying out other statutory functions, as well as in understanding and engaging with the public they serve. It is important that public authorities are able to make full and lawful use of this information for their statutory purposes. Much of it can be accessed without the need for RIPA authorisation; use of the internet prior to an investigation should not normally engage privacy considerations. But if the study of an individual's online presence becomes persistent, or where material obtained from any check is to be extracted and recorded and may engage privacy considerations, RIPA authorisations may need to be considered. The following guidance is intended to assist public authorities in identifying when such authorisations may be appropriate.

The internet may be used for intelligence gathering and/or as a surveillance tool. Where online monitoring or investigation is conducted covertly for the purpose of a specific investigation or operation and is likely to result in the obtaining of private information about a person or group, an authorisation for directed surveillance should be considered, as set out elsewhere in this code. Where a

person acting on behalf of a public authority is intending to engage with others online without disclosing his or her identity, a CHIS authorisation may be needed (paragraphs 4.10 to 4.16 of the Covert Human Intelligence Sources code of practice provide detail on where a CHIS authorisation may be available for online activity).

In deciding whether online surveillance should be regarded as covert, consideration should be given to the likelihood of the subject(s) knowing that the surveillance is or may be taking place. Use of the internet itself may be considered as adopting a surveillance technique calculated to ensure that the subject is unaware of it, even if no further steps are taken to conceal the activity. Conversely, where a public authority has taken reasonable steps to inform the public or particular individuals that the surveillance is or may be taking place, the activity may be regarded as overt and a directed surveillance authorisation will not normally be available.

As set out below, depending on the nature of the online platform, there may be a reduced expectation of privacy where information relating to a person or group of people is made openly available within the public domain, however in some circumstances privacy implications still apply. This is because the intention when making such information available was not for it to be used for a covert purpose such as investigative activity. This is regardless of whether a user of a website or social media platform has sought to protect such information by restricting its access by activating privacy settings.

Where information about an individual is placed on a publicly accessible database, for example the telephone directory or Companies House, which is commonly used and known to be accessible to all, they are unlikely to have any reasonable expectation of privacy over the monitoring by public authorities of that information. Individuals who post information on social media networks and other websites whose purpose is to communicate messages to a wide audience are also less likely to hold a reasonable expectation of privacy in relation to that information.

Whether a public authority interferes with a person's private life includes a consideration of the nature of the public authority's activity in relation to that information. Simple reconnaissance of such sites (i.e. preliminary examination with a view to establishing whether the site or its contents are of interest) is unlikely to interfere with a person's reasonably held expectation of privacy and therefore is not likely to require a directed surveillance authorisation. But where a public authority is systematically collecting and recording information about a particular person or group, a directed surveillance authorisation should be

considered. These considerations apply regardless of when the information was shared online.'

14. Scrutiny of investigatory bodies

The Investigatory Powers Commissioner's Office independently scrutinises the use of RIPA powers by the investigatory bodies that are subject to it.

The Commissioners will inspect Councils to ensure compliance with RIPA and can audit/review the Council's policies and procedures, and individual authorisations. Further detail can be found at https://www.ipco.org.uk/

15. Elected Members

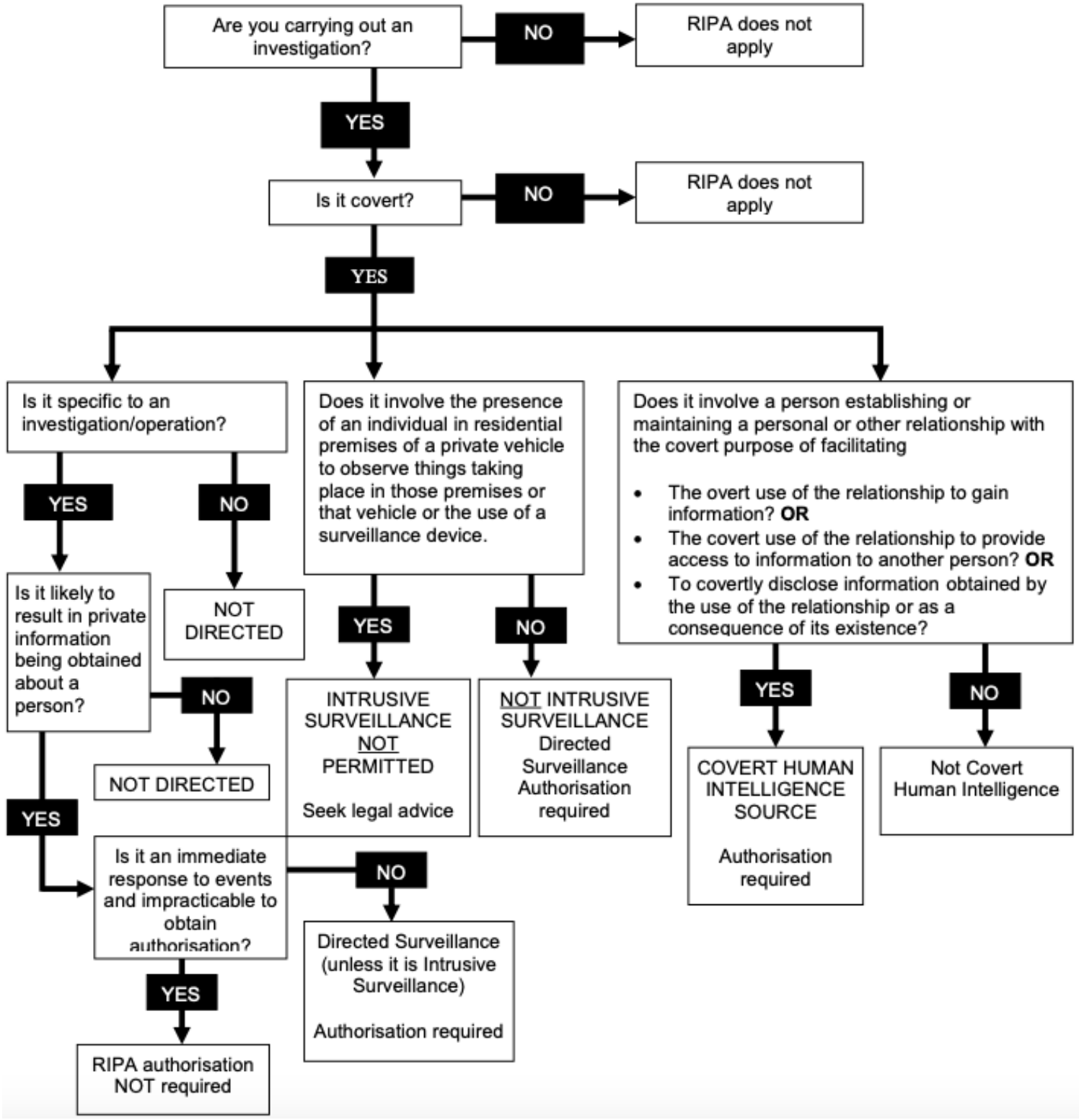
The elected members of the Council will review the council's use of RIPA and the authority's policy and guidance documents at least once a year. They will also be kept informed on a quarterly basis to ensure that it is being used consistently with the council's policy and that the policy remains fit for purpose. Members will not, however, be involved in making decisions on specific authorisations.

APPENDIX A

DIRECTED SURVEILLANCE

Regulation of Investigatory Powers Act 2000

Do you need Authorisation?



APPENDIX B

List of Authorised and Responsible Officers

RIPA Authorising Officers	Chief Executive, Deputy Chief Executive, Head of Operations, Head of Housing and Health Head of Planning
Authorising operations where confidential information may be obtained	Chief Executive only
CHIS Authorising Officer	Chief Executive only
CHIS Controller/Handler	Head of Operations Head of Housing and Health Head of Planning
Senior Responsible Officer	Head of Legal and Democratic Services

Please note:

- Where use of a CHIS is authorised, the head of the directorate carrying out the activity shall usually act as the CHIS Handler, with the CHIS Controller role being allocated by the Chief Executive.
- Authorising Officers must be "an assistant chief officer or investigations manager" or above.
- The Authorising Officers should not be directly involved in the investigation.

APPENDIX C i

Application Forms

Directed Surveillance

Application

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/application-directed-surveillanc?view=Binary

Review

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/review-directed-surveillance?view=Binary

Renewal

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/renewal-directed-surveillance?view=Binary

Cancellation

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/cancellation-directed-surveillan?view=Binary

Judicial Approval

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/local-authority-ripa-guidance/approval-order-form?view=Binary

APPENDIX C ii

Application Forms

Covert Human Intelligence Sources (CHIS)

Application

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/chis-application?view=Binary

Review

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/chis-review?view=Binary

Renewal

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/chis-renewal?view=Binary

Cancellation

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/chis-cancellation?view=Binary

APPENDIX C iii

Application Form for Communications Data

See Home Office website:

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/communications-data1.doc?view=Binary

APPENDIX D

Codes of Practice and Government Guidance

All current Government Codes of Practice are available on the Gov.uk website:

https://www.gov.uk/government/collections/ripa-codes#current-codes-of-practice

Protection of Freedom Act 2012 – Changes to provisions under the Regulation of Investigatory Powers Act 2000 (RIPA)

See Home Office website:

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/local-authority-ripa-guidance/local-authority-england-wales?view=Binary

Acquisition and Disclosure of Communications Data

See Home Office website:

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/code-of-practice-acquisition?view=Binary