The Regulation of Investigatory Powers Act 2000 (RIPA)

Policy Statement

To be approved by the Audit Committee 27 September 2022

Contents

Formatted Table

1 Introduction

1.1 The Regulation of Investigatory Powers Act 2000 (RIPA) regulates covert investigations by a number of bodies, including local authorities. It was introduced to ensure that individuals' rights are protected while also ensuring that law enforcement and security agencies have the powers they need to do their job effectively.

1.2 Wyre Borough Council is therefore included within the RIPA framework with regards to the authorisation of both Directed Surveillance and of the use of Covert Human Intelligence Sources and access to Communications Data.

1.3 The purpose of this guidance is to:-

- explain the scope of RIPA and the circumstances where it applies
- provide guidance on the authorisation procedures to be followed

1.4 The council has had regard to the Codes of practice produced by the Home Office in preparing this guidance and copies are attached at Appendix 4.

1.5 In summary, RIPA requires that when the council undertakes "directed surveillance" or uses a "covert human intelligence source" these activities must only be authorised by an officer with delegated powers when the relevant criteria is satisfied. Following changes made by the Protection of Freedoms Act 2012 all authorisations must be approved by a magistrate. If an officer requires access to communications data, the framework is provided by the Investigatory Powers Act 2016, and associated codes of practice. The authority must make the application through NAFN, the National Anti-Fraud Network, who by virtue of a collaborative agreement act as the authority SPOC. An extract from the Scheme of Delegation indicating the Authorising Officers is attached at Appendix 2.

1.6 Authorisation under RIPA gives lawful authority to carry out directed surveillance and the use of covert human intelligence source. Obtaining authorisation helps to protect the council and its officers from complaints of interference with the rights protected by Article 8 (1) of the European Convention on Human Rights and the UK which is now enshrined in English law through the Human Rights Act 1998. This is because the interference with the private life of citizens will be "in accordance with the law", and for a legitimate purpose. Provided activities undertaken are also "reasonable and proportionate" they will not be in contravention of Human Rights Legislation.

1.7 Authorising Officers and Investigators within the Local Authority are to note that RIPA does not extend powers to conduct intrusive Surveillance. Investigators should familiarise themselves with the provisions of the Code Of Practice on Directed Surveillance and Covert Human Intelligence Sources to ensure a good understanding of the limitation of powers within RIPA. Deciding when authorisation is required involves making a judgement. If you are in doubt, seek the advice of an Authorising Officer, if they are in doubt they will seek advice from the Senior Responsible Officer.

Formatted: Font: (Default) Arial, Font color: Red

Formatted: Font: Bahnschrift SemiBold, Font color: Red

Formatted: Font color: Red

Formatted: Indent: Left: -0.14 cm, Hanging: 0.5 cm

2 Directed Surveillance

2.1 **What is meant by Surveillance?**

"Surveillance'' Includes:

a) monitoring, observing or listening to persons, their movements, their conversations or their other activities or communication;

b) recording anything monitored, observed or listened to in the course of surveillance; and

c) surveillance by or with the assistance of a surveillance device.

2.2 **When is surveillance directed?**

Surveillance is 'Directed' for the purposes of RIPA if it is covert, but not Intrusive and is undertaken:

a) for the purpose of a specific investigation or a 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 is specifically identified for the purpose of the investigation or operation); and

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

2.3 **Surveillance becomes intrusive if the covert surveillance:**

a) Is carried out in relation to anything taking place on any **"residential premises''** or in any **"private vehicle'',** and;

b) involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device, or;

c) is carrying out by any means of a surveillance device in relation to anything taking place on any residential premises or in any private vehicle but is carried out without that device being present on the premises or in the vehicle, where the device is such that it consistently provides information of the same quality and detail as might be expected to be obtain from a device actually present on the premises or in the vehicle.

It should be noted that the council cannot authorise "intrusive surveillance''

2.4 Before any officer of the council undertakes any surveillance of any individual or individuals they need to assess whether the activity comes within RIPA. In order to do this the following key questions need to be

asked.

2.4.1 **Is the surveillance covert?**

Covert surveillance is that carried out in a manner calculated to ensure that subjects of it are unaware it is or may be taking place.

If activities are open and not hidden from the subjects of an investigation, the RIPA framework does not apply.

Examples of the surveillance are provided in the Code of Practice and are summarised in Appendix 3.

2.4.2 ***Is* it for the specific investigation or a specific operation?**

If officers are monitoring general activity in a street or car park whether covert or overt, then it is not covered by RIPA, as such general observation duties are part of the legislative functions of public authorities and are not pre-planned surveillance of a specific person or group of people.

2.4.3 **Is it in such a manner that is likely to result in the obtaining of private information about a person?**

"Private information'' is any information relating to a person's Private life or family life.

It is an issue of fact and degree, which has to be examined in each case.

Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that persons' activities may still result in the obtaining of private information. This is likely to be the case where that person has a reasonable expectation of privacy even though acting in public and where a record is being made by a public authority of that person's activities for the future consideration.

Example:
Officers of a local authority wish to drive past a café for the purpose of taking a photograph of the exterior. This is not likely to require a directed surveillance authorisation, as no private information about any person is likely to be obtained. However if the authority wish to establish a pattern of occupancy of the premises, the accumulation of information is likely to result in the obtaining of private information and a direct surveillance authorisation should be considered.

If it is likely that observation will not result in the obtaining of private information about a person, then it is outside RIPA.

2.4.4 **Otherwise than by way of an immediate response to events or circumstances where it is not reasonably practicable to get authorisation**

An example of an immediate response to something happening during the course of an observer's work which is unforeseeable would be a housing benefit fraud officer who conceals himself and continues to observe a person working who he knows to be claiming benefits and whom he comes across unexpectedly.

However, if as a result of that immediate response, a specific investigation subsequently takes place then it brings it within the RIPA framework.

2.4.5 **Surveillance – Direct or Intrusive?**

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 (high quality) surveillance device.

If the device is not in the premises or in the vehicle, it is only intrusive surveillance if it consistently produces information of the same quality as it if were.

Commercial premise and commercial vehicles are therefore excluded from intrusive surveillance.

High quality video monitoring or CCTV may run a significant risk of providing consistently high quality data "as if you were there" and therefore come within the definition of intrusive surveillance.

Matron boxes i.e. noise monitors, used by environmental health departments will not usually be covered. Usually they are stationed in a neighbouring property and do not provide evidence of the same quality as if the device was actually on the premises. Also the code of practice advises that in such circumstances the perpetrator would normally be regarded as having forfeited any claim to privacy.

The council is not authorised to carry out intrusive surveillance.

3 Covert use of Human Intelligence Source (CHIS)

3.1 A person is a **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 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.

3.2 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 that purpose.

3.3 A relationship is used covertly and an information obtained is disclosed covertly, if and only if it is used or as the case may be, 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.

3.4 An example by the Home Office is where intelligence suggests a local shop keeper is selling alcohol to underage customers and the local authority engages an employee to act as a juvenile in order to make a purchase of alcohol. In these circumstances any relationship, if established at all, is likely to be so limited, that the authority can conclude that an authorisation is unnecessary.

3.5 **Lay Witness**

Choose carefully how you chose to ask lay witnesses to gather information for you. For example, if a member of the public telephones to complain about noise nuisance caused by a neighbour. The lay witness is in a relationship with the neighbour already and is just passing on information to the council and would not be covered by RIPA. However the more the council tasks the lay witness to do something then you may inadvertently change them into a CHIS.

If you are in doubt seek advice from a senior Authorising Officer, and if they are in doubt they will seek advice from a Senior Responsible Officer.

3.6 **The use of Covert Human Intelligence Sources**

3.6.1 In practice it is most unlikely that it will ever be appropriate for the council to utilise a CHIS. However, in the event that it is ever considered, advice should be sought from the Senior Responsible Officer at an early stage. It is potentially possible that a council employee may be that of a source or the council may also use an external or professional source for the

purpose of obtaining information. Such persons may be a CHIS if he establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraphs b or c of paragraph 3.1.

3.6.2 Nothing in RIPA prevents material obtained by an employee acting as a source being used as evidence in court proceedings.

3.6.3 The Authorising officer must consider the safety and welfare of a CHIS acting a source, and the foreseeable consequences to others of the tasks they are asked to carry out. A risk assessment should be carried out before authorisation is given and considering what issues could be facing the security and welfare of a CHIS in relation to what they are being asked to do. This should take place before authorisation is granted, at any renewal, review and cancellation.

3.6.4 Before authorising the use of a CHIS as a source, the Authorising Officer should believe that the conduct/use including the likely degree of intrusion into the privacy of those potentially affected is proportionate to what the use or conduct of the source seeks to achieve. He should also take into account the risk of intrusion into the privacy of persons other than those who are directly the subjects of the operation or investigation (collateral intrusion) Measures should be taken, wherever practicable, to avoid unnecessary intrusion into the lives of those not directly connected with the operation.

3.6.5 Particular care should be taken in circumstances where people would expect a high degree of privacy or where, as a consequence of the authorisation, "confidential material" is likely to be obtained. (see definition of confidential material in Appendix 1) Special provisions relate to vulnerable individuals and juvenile services.

3.6.6 In additional to the usual authorisation process, the following management arrangements must be in place at all times in relation to the use of a CHIS:

1. There will be an appropriate officer of the council (handler) who has day-to-day responsibility for dealing with the CHIS, and for the security an welfare of the CHIS; and

2. there will be a second appropriate officer of the council who has general oversight of the use made of the CHIS, and who will have responsibility for maintaining an accurate and proper record about the source and tasks undertake (~~manager and recorder~~ controller or covert manager)

3.6.7 The CHIS forms contain appropriate boxes and prompts for ensuring the above is carried out.

4 Duration, Authorisations, Reviews Renewals and Cancellations

4.1 Duration

4.1.1 Authorisations lapse, if not renewed

4.1.1.1 within 12 months - from date of last renewal if it is for the conduct or use of a covert human intelligence source or;

4.1.1.2 in all other cases (i.e. directed surveillance) 3 months from the date of their grant or last renewal.

4.1.2 Directed Surveillance - Authorisation

4.1.2.1 For directed surveillance no officer shall grant an authorisation for the carrying out of directed surveillance unless he believes:

a. that an authorisation is **necessary** (on the one the ground detailed below) and

b. the authorised surveillance is **proportionate** to what is sought to be achieved by carrying it out.

4.1.2.2 An authorisation is necessary on the grounds stated below following the introduction of the Protection of Freedoms Act 2012:-

a. for the purpose of preventing or detecting conduct which constitutes/corresponds to a criminal offence that is punishable by a maximum custodial sentence of 6 months or more or;

b. constitutes an offence under s.146, 147or 147A of the Licensing Act 2003) - selling alcohol to children or;

c. selling tobacco to persons under 18 years of age (s.7 Children and Young Persons Act 1933).

4.1.2.3 The Authorising Officer should be set out, in its own words, why he believes the activity is necessary and proportionate. A bare assertion is insufficient. The onus is therefore on the person authorising such surveillance to satisfy themselves it is:

a. necessary for the ground stated above and be able to demonstrate the reasons why it is necessary and;

b. proportionate to its aim.

This involves balancing the seriousness of intrusion into the privacy of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative and operational terms.

The authorisation will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an

expected benefit to the investigation or operation and should not be disproportionate or arbitrary.

The following elements of proportionally should therefore be considered:

- Balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;

- Explaining how and why the methods will cause the least possible intrusion on the subject and others;

- Considering whether the activity is an appropriate use of the legislation and a reasonable way having considered all reasonable alternatives of obtaining the necessary result;

- Evidencing as far as reasonably practicable, what other methods had been considered and why they were not implemented.

It is important therefore that all officers involved in surveillance are fully aware of the extent and limits of the authorisation.

The Code of Practice give an example of an individual suspected of carrying out a series of criminal damage offences at a local shop after a dispute with the owner. It suggested that a period of directed surveillance should be conducted against him to record his movements and activities for the purpose of preventing or detecting crime. Although these are legitimate grounds on which directed surveillance may be conducted, the Home Office Code states that it is unlikely the interference with privacy will be proportionate in the circumstances of the particular case. In particular the obtaining of private information on the individuals daily routine is unlikely to be necessary or proportionate in order to investigate the activity of concern. Instead, other less intrusive means are likely to be available, such as overt observation of the location in question until such time as a crime may be committed.

4.1.2.4 In order to ensure Authorising Officers have sufficient information to make an informed decision it is important that detailed records are maintained. The applicant in completing the forms must provide facts and evidence.

4.1.2.5 It is also sensible to make any authorisation sufficiently wide enough to cover the means required as well as being able to prove effective monitoring of what is done against what is authorised.
Authorisations must be in writing. The standard forms to be used can be accessed via the council's intranet.

4.1.2.6 **IMPORTANT NOTE: THE PROTECTION OF FREEDOMS ACT 2012 INTRODUCES A REQUIREMENT FOR MAGISTRATE APPROVAL FOR ALL RIPA AUTHORISATIONS FROM 1 NOVEMVER 2012. ACCORDINGLY AUTHORISATIONS CANNOT TAKE EFFECT UNTIL SUCH TIME AS A JP HAS MADE AN ORDER APPROVING THE AUTHORISATION I.E. A GRANT OR RENEWAL.**

The procedure and application process is set out in Appendix 8. It is important that you seek advice from the Senior Responsible Officer before making the application for judicial approval.

4.1.2.7 Any Authorising officer proposing to approve an application for the use of directed surveillance, or for the use of CHIS must immediately inform the Senior Responsible Officer, who will then make arrangements for an application to be made to the Magistrates' Court.

4.1.2.8 In such circumstances the council will be required to make an application, without giving notice to the Magistrates Court. The Magistrates will give approval if and only if, at the date of the grant of authorisation or renewal of an existing authorisation they are satisfied that:

a) there were reasonable grounds for believing that obtaining the covert surveillance or use of a human covert intelligence source was reasonable and proportionate and that these ground still remain

b) the "relevant conditions" were satisfied in relation to the authorisation.

Relevant conditions include that:

1. the relevant person was a designated as an Authorising Officer.

2. it was reasonable and proportionate to believe that using covert surveillance or a CHIS was necessary and that the relevant conditions have been complied with.

3. the grant or renewal of any authorisation or notice was not in breach of any restrictions imposed under section 25 (3) of RIPA (restrictions on the rank of the person granting the authorisation)

4. any other conditions provided for by an order made by the Secretary of State were satisfied.

If the Magistrates' Court refuses to approve the grant or renewal of the authorisation, it may make an order to quash that authorisation. However the court may not exercise its power to quash the authorisation unless the council has had at least two business days from the date of refusal in which to make any representations.

4.1.3 **Reviews**

4.1.3.1 Authorising Officers are responsible for ensuring that authorisations undergo timely reviews and are cancelled promptly after directed surveillance activity is no longer necessary.

4.1.3.2 It is recommended that regular reviews be undertaken to see if the need for the surveillance is still continuing. Results of reviews should be recorded in the Central Register of Authorisations (see paragraph 7) Reviews should be more frequent when access is more confidential information or collateral intrusion is involved. Review frequency should be

as often as the Authorising Officer deems necessary or practicable.

4.1.3.3 Each Authorising Officer will therefore determine in each case how often authorisations should be reviewed. It is recommended that they ensure records of the review be supplied on the relevant form. Copies should be sent to the Senior Responsible Officer to keep the Central Register up to date.

4.1.4 **Renewals**

4.1.4.1 An Authorising Officer may renew an authorisation before it would cease to have effect if it is necessary for the authorisation to continue for the purpose for which it was given. A renewal of the authorisation in writing can be made for up to 3 months. Applications for renewal should detail how any times an authorisation has been renewed; significant changes to the original application for authority; reasons why it is necessary to renew; content, value of the information obtained so far and results of regular reviews of the investigation or operation.

4.1.4.2 Each application to renew should be made at least 7 days before the authorisation is due to expire on the relevant form. A record of the renewal should be kept within the applying service and supplied centrally to the Senior Responsible Officer to be placed in the Central Register.

IMPORTANT NOTE: FROM 1 NOVEMBER 2012 RENEWALS CANNOT TAKE EFFECT UNTIL SUCH TIME AS A MAGISTRATE HAS MADE AN ORDER APPROVING THE RENEWAL.

4.1.5 **Cancellations**

4.1.5.1 All Authorisations, including renewals should be cancelled if the need for surveillance is no longer justified. This will occur in most cases where the purpose for which the surveillance was required has been achieved.

4.1.5.2 Requesting officers should ensure they inform authorising officers if this is the case before the next review. If, in opinion of the Authorising Officer at the next review the need for surveillance is no longer justified it must be cancelled.

4.1.5.3 The cancellation forms will be used to record a cancellation, and the Authorising Officer will ensure the original cancellation has been sent to the Senior Responsible Officer or nominated reprehensive to update the Central Register.

4.2 **Covert use of Human Intelligence Sources**

4.2.1 **Authorisation**

4.2.1.1 The same principles as set out in paragraphs 4.1.2.1 and 4.1.2.2 apply to CHIS except the ground on which a CHIS can be authorised, which remains unaltered by the Protection of Freedoms Act 2012.

A CHIS authorisation can only be approved where it is necessary for the purpose of preventing or detecting crime, or preventing disorder.

A CHIS authorisation can last for up to 12 months.

4.2.1.2 The conduct so authorised is any conduct that:

a) is comprised in any such activities involving the conduct or use of a ~~covert human intelligence source~~CHIS, as are specified or described in the authorisation;

b) relates to the person who is specified or described as the person whose actions as a ~~covert human intelligence source~~CHIS the authorisation relates; and

c) is carried out for the purpose of, or in connection with the investigation or operation so specified or described.

4.2.1.3 In order to ensure that Authorising Officers have sufficient information to make an informed decision it is important that detailed records are maintained.

It is also sensible to make any authorisation sufficiently wide enough to cover all the means required as well as being able to prove effective monitoring of what is done against the authorised.

4.2.2 ***Renewals/Reviews***

4.2.2.1 Similar provisions apply for a CHIS except that a renewal here can last for a further 12 months, a review must have been carried out on the use of the source and an application should only be made to renew when the initial authorisation period is drawing to an end. Applications to renew a CHIS also should contain use made of the source and tasks given to the source during the previous authorised period and the information obtained.

IMPORTAMT NOTE: FROM 1 NOVEMBER 2012 AUTHORISATIONS CANNOT TAKE EFFECT UNIL SUCH TIME AS A MAGISTRATE HAS MADE AN ORDER APPROVING THE AUTHORISATION I.E A GRANT OR RENEWAL.

4.2.3 **Cancellations**

4.2.3.1 The same principles as Directed Surveillance apply.

4.2.3.2 Separate forms have been devised to applications to authorise, review, renew and cancel a CHIS. These can be accessed via the Councils intranet.

5 Communications Data

~~5.1~~ ~~**Acquisition of Communications Data**~~

5.1 Before considering submitting an application for the acquisition of communications data, all officers must first refer the matter to the Senior Responsible Officer.

5.2 Communications Data ('CD') is the 'who', 'when' and 'where' of a communication, but not the 'what' (i.e. the content of what was said or written). Local Authorities are not permitted to intercept the content of any person's communications.

5.3 Part 3 of the Investigatory Powers Act 2016 (IPA) replaced part 1 chapter 2 of RIPA in relation to the acquisition of communications data (CD) and puts local authorities on the same standing as the police and law enforcement agencies. Previously local authorities have been limited to obtaining subscriber details (known now as "entity" data) such as the registered user of a telephone number or email address. Under the IPA, local authorities can now also obtain details of in and out call data, and cell site location. This information identifies who a criminal suspect is in communication with and whereabouts the suspect was when they made or received a call, or the location from which they were using an Internet service. This additional data is defined as "events" data.

5.4 A new threshold for which CD "events" data can be sought has been introduced under the IPA as "applicable crime". Defined in section 86(2A) of the Act this means: an offence for which an adult is capable of being sentenced to one year or more in prison; any offence involving violence, resulting in substantial financial gain or involving conduct by a large group of persons in pursuit of a common goal; any offence committed by a body corporate; any offence which involves the sending of a communication or a breach of privacy; or an offence which involves, as an integral part of it, or the sending of a communication or breach of a person's privacy. Further guidance can be found in paragraphs 3.3 to 3.13 of CD Code of Practice.

5.5 Finally, the IPA has also removed the necessity for local authorities to seek the endorsement of a Justice of the Peace when seeking to acquire CD. All such applications must now be processed through NAFN and will be considered for approval by the independent Office of Communication Data Authorisation (OCDA). The transfer of applications between local authorities, NAFN and OCDA is all conducted electronically and will therefore reduce what can be a protracted process of securing an appearance before a Magistrate or District Judge (see local authority procedures set out in paragraphs 8.1 to 8.7 of the CD Code of Practice).

~~The Regulation of Investigatory Powers (Communications Data) Order 2010 replaced the earlier 2003 order which gave local authorities the powers set out within RIPA to access communications data. The 2010 Order raised the seniority of the Authorising Officers in local authorities to a Director, Head of service, Manager or equivalent.' Communications data~~

Formatted: Indent: Left: 2 cm

includes information relating to the use of a communications service but it does not in include the contents of the communications itself. Communications data can be split into three types; "traffic data" i.e. where a communication was made from, to whom and when; "service data" is the use made by the service by any person eg itemised telephone records; and "subscriber data" i.e. any other information that is held or obtained by an operator on a person they provide a service to. Local authorities are allowed to access "service data" and "subscriber data"; they are not allowed to access "traffic data".

5.2 **Authorisation**

The Order permits access to communications data, by local authorities only where it is necessary for the purpose of preventing or of detecting crime or preventing disorder. As with surveillance, access to communications data should only be authorised where it is proportionate to the objectives the Council is seeking to achieve. It should not be authorised where less intrusive means can be used to further an investigation

Formatted: Indent: Left: 0 cm

5.3 **Alternative methods for authorisation**

Formatted: Indent: Left: 0 cm

Access to communications data may be authorised in two ways; either (a) through an authorisation by an Authorising Officer which would allow the authority to collect or retrieve data itself, or (b) by a notice given to a postal or telecommunications operator requiring that operator to collect or retrieve the data provided it to the local authority.

5.4 **Application**

Formatted: Indent: Left: 0 cm

Application will be made by the investigating officer and submitted to a Single Point of Contact (SPOC) who will either accept or reject the application. If the SPOC accepts the application he will forward it together with a SPOC report and a draft notice (where appropriate) to an Authorising Officer for authorisation.

If the Authorising Officer accepts the application, it will need to be approved by a magistrate before the forms are returned to the SPOC and the SPOC will deal with the postal or telecommunications operator directly. The SPOC will also advise investigating officers and Authorising Officers on whether an authorisation or notice is appropriate in the circumstances.

Although it's unlikely that the Council will access communications data, in the event that it did, the Council would appoint a nominated SPOC and NAFN, (National Anti-Fraud Network) who have received training on a course recognised by the Home Office.

Formatted: Indent: Left: 1.27 cm

Authorising officers

Authorising Officers for the purpose of communications data will be the same as for directed surveillance and CHIS's

~~IMPORTANT NOTE: FROM 1NOVEMBER 2012 AUTHORISATIONS CANNOT TAKE EFFECT UNTIL SUCH TIME AS A MAGISTRATE HAS MADE AN ORDER APPROVING THE AUTHORISATION. SEE PARAGRAPHS 4.1.2.6 – 4.1.2.8 ABOVE~~

Formatted: Indent: Left: 1.27 cm, First line: 0 cm

6 Other factors to consider

Particular consideration should be given to **collateral intrusion** i.e. the risk of intrusion into the privacy of those not directly the targets of the investigation. Measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the privacy of those who are not the intended subjects of the surveillance activity. Where such collateral intrusion is unavoidable, the activities may still be authorised, provided this intrusion is considered proportionate to what is sought to be achieved. The same proportionality test, as outlined above apply to the likelihood of collateral intrusion as to intrusion into the privacy of the intended subject if the surveillance. Such collateral intrusion or interference would be a matter of greater concern in cases where there are special sensitivities, for example in cases of premises used by lawyers or for any form of medical or professional counselling or therapy.

6.2 An application for an authorisation should include an assessment of the risk of any collateral intrusion or interference. The Authorising Officer will take this into account, particularly when considering the proportionality of the surveillance.

6.3 Those carrying out the covert surveillance should inform the Authorising Officer if the operation/investigation unexpectedly interferes with the privacy of individuals who are not the original subject of the investigation or covered by an authorisation in some other way. In some cases the original authorisation may not be sufficient and consideration should be given to whether a separate authorisation is required.

6.4 Any person giving authorisation will also need to be aware of particular sensitivities in the local community where the surveillance is taking place or of similar activities being undertaken by other public authorities which could impact on the deployment of surveillance.

Confidential Material

6.5 RIPA does not provide any special protection for **"confidential material"** (see definitions in Appendix 1) Nevertheless, such material is particularly sensitive, and is subject to additional safeguards. In cases where the likely consequence of the conduct of a source would be for any person to acquire knowledge of confidential material, the deployment of the source should be subject to a special authorisation. i.e. by the Chief Executive.

6.6 In general, any application for an authorisation which is likely to result in the acquisition of confidential material should include an assessment of how likely it is that confidential material will be acquired. Special care should be taken when the target of the investigation is likely to be involved

in handling confidential material. Such applications should only be considered in the exceptional and compelling circumstances with full regard to the proportionality issues this raises.

6.7 The following general principles apply to confidential material acquired under authorisations:

- Those handling material from such operations should be altered to anything that may fall within the definition of confidential material where there is doubt as to whether the material is confidential, advice should be sought from the Senior Responsible Officer before further dissemination takes place;

- Confidential material should not be retained or copied unless it is necessary for a specific purpose;

- Confidential material should be disseminated only where an

  appropriate officer (having sought advice from the Senior Responsible Officer) is satisfied that it is necessary for a specific purpose;

- The retention or dissemination of such information should be accompanied by a clear warning of its confidential nature. It should be safeguarded by taking reasonable steps to ensure that there is no possibility of it becoming available, or its content being known, to any person whose possession of it might prejudice any criminal or civil proceedings related to the information.

- Confidential material should be destroyed as soon as it is no longer necessary to retain it for a specified purpose.

6.8 In the case of confidential information a higher level of authorisation is Required. Therefore where authorisation is sought to carry out surveillance in respect in respect of communications subject to legal professional privilege, or containing confidential personal information or confidential journalistic material, the Chief Executive must sign the authorisation.

Joint Working

6.9 In cases of joint working, where one agency is acting on behalf of another, usually the tasking agency can obtain or provide the authorisation i.e. if the Council has been tasked by the Police to assist in a covert surveillance operation, they should get the authorisation, which would the cover the Council. But advice should be sought from the Senior Responsible Officer prior to any arrangements being agreed.

Handling and Disclosure of Materials

6.10 Authorising Officers are reminded of the guidance relating to the retention and destruction of confidential material as described in paragraph 6.7

above.

6.11 Applications and associated reviews, renewals and cancellations for directed surveillance shall be centrally retrievable for a period of 5 years Where it is believed that the records could be relevant to pending or future criminal proceedings, they should be retained for a suitable further period, commensurate to any subsequent review.

6.12 Authorising officers must ensure compliance with the appropriate data protection requirements and the relevant codes of practice in the handling and storage of material. Where material is obtained by surveillance, which is wholly unrelated to a criminal or other investigation or to any person who is the subject if the investigation and there is no reason to believe it will be relevant to future civil or criminal proceedings, it should be destroyed immediately. Consideration is whether or not unrelated material should be destroyed is the responsibility of the Authorising Officer. If in doubt advice should be sought from the Senior Responsible Officer.

6.13 There is nothing in RIPA that prevents material obtained through the proper use of the authorisation procedures from being used in other investigations. However the use outside the Council, of any material obtained by means of covert surveillance and other than in pursuance of the ground, on which is was obtained, should be authorised only in the most exceptional circumstances. Advice should be sought from the Senior Responsible Officer.

7 Central Register of Authorisation

7.1 The RIPA code of practice requires a central register of all authorisations to be maintained. The Legal Section maintains this register.

7.2 Whenever an authorisation is authorised, renewed, reviewed or cancelled the Authorising Officer must send the signed original authorisation to the Senior Responsible Officer or nominated representative. Receipt is the form will be acknowledged.

7.3 The Central Register will contain the following information:

- the type and date of authorisation;
- the name and grade of the Authorising Officer;
- a unique reference number for the investigation or operation;
- the title of the investigation/operation, and a brief description and names of the subjects, if known;
- if an authorisation is renewed, when and the name and designation of the Authorising Officer;
- if confidential information is likely to be a consequence of the investigation or operation;
- the date the authorisation was cancelled;
- the date of magistrates court approval.

7.4 The legal section will securely retain the original authorisations and maintain the Central register. Authorisations should only be kept for a

maximum of 5 years from the end of an authorisation. Once the investigation is closed (bearing in mind cases may be lodged sometime after the initial work) the records held by the department should be disposed of in an appropriate manner (e.g. Shredded)

8 Codes of Practice

8.1 There are Home Office codes of practice and Office of Surveillance Commissioners (OSC) Guidance that expand on this policy statement and copies are attached at Appendices 4 and 6. The codes also list General Best Practices, which should be followed where at all possible.

8.2 The codes do not have the force of statute, but are admissible in evidence in any criminal and civil proceedings. As stated in the codes, "if any provision of the code appears relevant to a question before any Court or tribunal considering any such proceedings, or to the tribunal established under RIPA, or to one of the commissioners responsible for overseeing the powers conferred by RIPA, it must be taken into account''

8.3 Staff should refer and familiarise themselves with the Home Office Code of Practice and OSC Guidance for supplementary guidance.

8.4 Authorising Officers and the Senior Responsible Officer should also familiarise themselves with the Procedures and Guidance document produced by the OSC attached at Appendix 6.

9 Benefits of obtaining Authorisation under RIPA

9.1 **Authorisation of surveillance and human intelligence sources**

RIPA states that

- if authorisation confers entitlement to engage in a certain conduct and;
- the conduct is in accordance with the authorisation, then;
- "it shall be lawful for all purposes"

However, the corollary is not true – i.e. if you do not obtain RIPA authorisation it does not make any conduct unlawful (e.g. use of intrusive surveillance by local authorities). It just means that you cannot take advantage of any of the special RIPA benefits.

9.2 RIPA states that a person shall not be subject to any civil liability in relation to any conduct of his which:

a) is incidental to any conduct that is lawful by virtue of an authorisation and;

b) is not itself conduct for which an authorisation is capable of being granted under a relevant enactment and might reasonably be expected to have been sought in the case in question.

10 Scrutiny and Tribunal

10.1 The Investigatory Powers Commissioners Officer (IPCO) has taken over the inspection and oversight functions on RIPA which was previously carried out by the Surveillance Commissioner's Office. The IPCO and his assistants will continue to ensure RIPA compliance by conducting a programme of inspections of Local Authorities. As a generality, they aim to inspect each council in England, Wales and Scotland once every three years but have introduced remote desktop inspections what a local authority has significantly reduced or stopped using their powers under RIPA and when there are no apparent significant compliance concerns. However, a desktop inspection will always be followed by an onsite inspection.

10.2 RIPA provides for the establishment of a tribunal to consider and determine complaints made under RIPA, and persons aggrieved by a local authority's conduct e.g. directed surveillance can make complaints to the tribunal. The forum hears applications on a judicial review basis. Claims should be brought within one year unless it is just and equitable to extend that.

10.3 The tribunal can order, among other things, the quashing or cancellation of any authorisation and can order destruction of any records or information obtained by such authorisation, and records of information held by any public authority in relation to any person. The council is, however, under a duty to disclose or provide to the tribunal all documents they require if:

- A council Officer has granted any authorisation under RIPA.
- Council employees have engaged in any/all conduct as a result of such authorisation.
- A disclosure notice requirement is given.

11 Covert Surveillance of Social Networking Sites (SNS)

11.1 The growth of the internet, and the extent of the information that is now available online, presents new opportunities for the Council to view or gather information which may assist it in preventing or detecting crime or carrying out any other statutory functions, as well as understanding and engaging with the public is serves. It is important that the Council is able to make full and lawful use of this information for its statutory purposes. Much of it can be assessed without the need for RIPA authorisation (use of the internet prior to an investigation should not normally engage privacy considerations)

11.2 If the study of an individual’s online presence becomes persistent or where material obtained from any check is to be extracted and recorded any may engage privacy considerations, RIPA authorisations many need to be considered.

11.3 Officers are required to follow the processes outlined in Appendix 11,

when viewing social media sites in investigations or to gather information.

11.4 The following guidance taken from the Home Office Covert Surveillance and Property Interface Revised Code Of Practice (August 2018) is intended to assist the council in identifying when such authorisations may be appropriate.

11.5 The internet may be used for intelligence gathering and/or as a surveillance tool.

11.6 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 and authorisation for directed surveillance should be considered, as set out elsewhere in this policy

11.7 Where an officer is intending to engage with others online without disclosing his or her identity, a CHIS authorisation may be needed. However, it is considered that it is most unlikely that it will ever be appropriate for the council to utilise a CHIS.

11.8 In deciding whether online surveillance should be regarded a covert, consideration should be given to the likelihood of the subject(s) knowing that the surveillance is or maybe 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 the council 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 required.

11.9 Depending on the nature of 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.

11.10 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 the council 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 hole a reasonable expectation of privacy in relation to the information.

11.11 Whether the council interferes with a person's private life includes a consideration of the nature of the councils 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) it's 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 council 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.

Example 1:
An officer undertakes a simple internet source on a name address or telephone number to find out whether a subject of interest has an online presence. This is unlikely to need an authorisation. However, if having found an individual's social media profile or identity is decided to monitor it or extract information from it for retention in a record because it is relevant to an investigation or operation. authorisation should then be considered.

Example 2:
An officer makes an initial examination of an individual's online profile to establish whether they are of relevance to an investigation. This is unlikely to need an authorisation. However, if during that visit it is intended to extract and record information to establish a profile including information such as identity, pattern of life, habits, intentions or associations, it may be advisable to have in place an authorisation even for that single visit. (As set out in the following paragraph, the purpose of the visit may be relevant as to whether an authorisation should be sought)

Example 3:
An officer undertakes general monitoring of the internet in circumstances where it is not part of a specific, ongoing investigation or operation to identify themes, trends possible indicators or criminality or other factors that may influence operational strategies or deployments. This activity does not require RIPA authorisation, however when this activity leads to the discovery of previously unknown subjects of interest, once it is decided to monitor those individuals as part of an ongoing operation or investigation authorisation should be considered.

11.12 In order to determine whether a directed surveillance authorisation should be sought for accessing information on a website as part a covert investigation or operation, it is necessary to look at the intended purpose and scope of the online activity it is proposed to undertake factors that should be considered in establishing whether a directed surveillance authorisation is required to include:

- Whether the investigation or research is directed towards an

individual or organisation;

- Whether it is likely to result in obtaining private information about a person or group of people;
- Whether it is likely to involve visiting internet sites to build up an intelligence picture or profile;
- Whether the information obtained will be recorded and retained;
- Whether the information is likely to provide and observer with a pattern of lifestyle;
- Whether the information is being combined with other sources of information or internet searches carried out by a third party on behalf of a public authority, or with the use of a search tool, many still require a directed surveillance authorisation.
- Intelligence, which amounts to information relating to a person's private life;
- Whether the investigation or research is part of an ongoing piece of work involving repeated viewing of the subject(s);
- Whether it is likely to involve identifying and recording information about third parties, such as friends and family members of the subject of interest, or information posted by third parties, that may include private information and therefore constitute collateral intrusion into the privacy of these third parties;
- Internet searches carried out by a third party on behalf of a public authority, or with the use of a search tool, may still require a directed surveillance authorisation.

Example:
Officers using automated monitoring tools to search for common terminology used online for illegal purposes will not normally require a directed surveillance authorisation. Similarly, general analysis of data either directly or through a third party for predictive purposes (e.g. identifying crime hotspots or analysing trends) is not usually directed surveillance. In such cases, the focus on individuals or groups is likely to be sufficiently cursory that it would not meet the definition of surveillance. But officers should be aware of the possibility that broad thematic research may evolve, and that authorisation may be appropriate at the point where it begins to focus on specific individuals or groups. If specific names or other identifiers of an individual or group are applied to the search or analysis, an authorisation should be considered.

12 Conclusion

12.1 If you can carry out investigations in an obviously overt way so that it does not compromise what you are trying to achieve then you need to consider RIPA and you are advised to take a broad view and interpretation of your activities. If you are in doubt you can seek advice from the Senior Responsible Officer and remember if there is any doubt then it is usually safer to get authorisation.

APPENDIX 1

Definitions from the 2000 Act

- "**RIPA"** means the Regulation of Investigatory Powers Act 2000.
- "SRO" means Senior Responsible Officer
- "CHIS" means Covert Human Intelligence Sources
- "**Confidential material"** consists of:

  a) Matters subject to legal privilege;

  b) Confidential personal information; or

  c) Confidential journalistic material.

- **"Matters subject to legal privilege"** includes both oral and written communications between a professional legal adviser and his/her client or any person representing his/her client, made in connection with the giving of legal advice to the client or in contemplation of legal proceedings and for the purposes of such proceedings, as well as items enclosed with or referred to in such communications. Communications and items held with the intention of furthering a criminal purpose are not matters subject to legal privilege (see Note A Below).

- **"Confidential personal information"** is information held in confidence concerning an individual (whether living or dead) who can be identified from it, and relating:

  a) to his/her physical or mental health or;

  b) to spiritual counselling or other assistance given, and;

which a person has acquired or created in the course of any trade, business profession or other occupation or for the purpose of any paid or unpaid office (see Note B below) it includes both oral and written information and also communications as a result of which personal information is acquired or created. Information is held in confidence if:

  c) it is held subject to an express or implied undertaking to hold it in confidence, or;

  d) it is subject to a restriction on disclosure or an obligation of secrecy contained in existing or future legislation.

- **"Confidential Journalistic Material"** includes material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence, as well as communications resulting in information being acquired for the purpose of journalism and held subject to such an undertaking.

- **"covert Surveillance**" means surveillance which 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;

- **"Authorising Officer"** means a person designated for the purpose of RIPA to grant authorisations for directed surveillance.

Note A *Legally privileged communications will lose their protection if there is evidence, for example, that the professional legal advisor is intending to hold or use them for a criminal purpose; privilege is not lost if a professional legal advisor is properly advising a person who is suspected of having committed a criminal offence. The concept of legal privilege shall apply to the provision of professional legal advice by any agency or organisation*

Note B *Confidential personal information might for example, include consultations between a health professional or a professional counsellor and a patient or client, or information from a patient's medical records.*

APPENDIX 2

Extract from Part 7 of the Councils Constitution - Management Structure and Scheme of Delegation

Scheme of Delegation to Officers -

All delegations to officers are subject to the following general conditions:

(2) In the absence of the Chief Executive the functions of the Chief Executive will be the responsibility of any of the Corporate Directors. ~~either one of the three Services Directors~~

Formatted: Indent: Left: 1.88 cm, Hanging: 0.12 cm

Executive functions Delegated to the Chief Executive (8~~7~~) To Provide the necessary authorisations in respect of surveillance in accordance with the Regulation of Investigatory Powers Act 2000, where confidential information is involved or where authorisation is sought for the employment of a juvenile or vulnerable Covert Human Intelligence Source (CHIS).

Executive Functions Delegated to the ~~Service~~ Corporate Directors

(2) To act as authorising officers for the purpose of the Regulation of Investigatory Powers Act 2000 and Protection of Freedoms Act 2012.

Executive Functions Delegated to the Legal Services Manager

(3) To act as the Senior Responsible Officer for the purpose of Part ll of the Regulation of Investigatory Powers Act 2000.

(5~~4~~) To make an application to a justice of the Peace in accordance with the Protection of Freedoms Act 2012, seeking an order approving the grant or renewal of a RIPA authorisation or notice and to represent the Council in making such an application.

Executive Functions Delegated to Revenues Manager and Senior Compliance Officers~~Fraud and Compliance Manager and Fraud Investigation Officers~~

(1) To make an application to a justice of the Peace, in accordance with the Protection of Freedoms Act 2012, seeking an order approving the grant or renewal of a RIPA authorisation or notice and to represent the council in making such an application.

(3) Power to carry to carry out surveillance which is governed by the Regulation of Investigatory Powers Act 2000 as agreed by an authorising officer.

APPENDIX 3

Examples of Surveillance

Examples of different types of surveillance	**Examples**
Surveillance that does **not** require RIPA Authorisation.	- Council Officers on patrol who conceal themselves to observe suspicious persons that they come across in the course of a routine patrol. - Signposted Town Centre CCTV cameras (in normal use) -Recording noise coming from outside the premises after the occupier has been warned that this will occur if the noise persists. - Sampling purchases (where the officer behaves no differently from a normal member of the public) - Dog warden in uniform on patrol on park, street or van. - Food Safety or Health and Safety Inspections. -General observational duties not specifically targeted/planned or considered direct surveillance. - CCTV cameras providing general traffic, crime or public safety information. - Covert surveillance of an employee who is suspected by his employer of undertaking additional duties in breach of discipline regulations, as it does not relate to the discharge of the Employers core functions.
Covert directed Surveillance must be RIPA authorised	Officers follow/observe an individual or individuals over a period, to establish whether s/he is working when claiming benefit provided the conduct constitutes/corresponds to a criminal offence punishable with at least 6 months imprisonment.
Surveillance that is not intrusive.	**-** An observation post outside residential premises, which provides a limited view compared to that which would be achievable from within the premises.
Intrusive - **Council cannot do this!**	- Planting a listening or other device in a person's home or in their private vehicle - use of a zoom lens outside residential premises, which consistently archives imagery of the same quality as that which would be visible from within the premises.