SOLIHULL METROPOLITAN BOROUGH COUNCIL

REGULATION OF INVESTIGATORY POWERS ACT 2000 AS AMENDED

CORPORATE PROCEDURE

Nick Page
Chief Executive

November 2022

CONTENTS

1. Summary

Solihull MBC is committed to building a fair and safe community for all by ensuring the effectiveness of laws designed to protect individuals, businesses, the environment and public resources.

Solihull MBC recognises that most organisations and individuals appreciate the importance of these laws and abide by them. The Council will use its best endeavours to help them meet their legal obligations without unnecessary expense and bureaucracy.

At the same time the Council has a legal responsibility to ensure that those who seek to flout the law are the subject of firm but fair enforcement action. Before taking such action, the Council may need to undertake covert surveillance of individuals and/or premises to gather evidence of illegal activity.

The Council's Surveillance Policy sets out the framework for the authorisation of surveillance activities throughout each section of the Council. All staff whose functions may involve covert surveillance or the use or conduct of a covert human intelligence source must be aware of the Council's policy and procedure.

At no time should the Council undertake any surveillance that interferes with any private property. Placing tracking devices on a subject's vehicle or person are not authorised for local authorities and must not be used. If anyone has any doubt under RIPA, this document or any related legal provisions, please consult with the RIPA co-ordinator at the earliest possible opportunity.

This procedure, the Council's Surveillance Policy and all related documents such as source legislation and statutory codes of practice are available for inspection and download on the home office website.

Covert Surveillance is carried out in a manner calculated to ensure that the person subject to the surveillance is unaware of it taking place. (Section 26(9)(a) of RIPA). It cannot, however, be "necessary" if there is reasonably available an overt means of finding out the information desired.

RIPA regulates two types of covert surveillance, (Directed Surveillance and Intrusive Surveillance) and the use of Covert Human Intelligence Sources (CHIS).

Most of the surveillance carried out by the Council will be done overtly – there will be nothing secretive, clandestine or hidden about it. In many cases, Officers will be behaving in the same way as a normal member of the public and/or will be going about Council business openly.

Directed Surveillance is defined in Section 26(2) of the 2000 Act as surveillance which is covert, but not intrusive, and undertaken for the purposes of a specific investigation, in such a manner as is likely to result in the obtaining of private information about a person and otherwise than by way of an immediate response to events or circumstances.

Intrusive surveillance is defined as surveillance that is carried out in relation to anything taking place on any residential premises or in any private vehicle and involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device. (Local Authorities are not permitted to carry out any intrusive surveillance).

Private information in relation to a person includes any information relating to his private and family life, his home and his correspondence. The fact that covert surveillance occurs in a public place or on business premises does not mean that it cannot result in the obtaining of private information about a person.

2. Procedure

Solihull MBC shall ensure that covert surveillance is only undertaken where it complies fully with all applicable laws in particular the:

Human Rights Act 1998
Regulation of Investigatory Powers Act 2000/Surveillance Codes as amended
Protection of Freedoms Act 2012
General Data Protection Regulation 2018 (GDPR)

The Council shall, in addition, have due regard to all official guidance and codes of practice particularly those issued by the Home Office, Investigatory Powers Commissioners Office (IPCO), the Security Camera Commissioner and the Information Commissioner.

In particular the following guiding principles shall form the basis of the all covert surveillance activity undertaken by the Council:

* Shall only be undertaken where it is absolutely necessary to achieve the desired aims.

* Shall only be undertaken where it is proportionate to do so and in a manner that it is proportionate.

* Adequate regard shall be had to the rights and freedoms of those who are not the target of the covert surveillance.

* All authorisations to carry our covert surveillance shall be granted by designated authorising officers.

* Covert surveillance [regulated by RIPA] shall only be undertaken after obtaining judicial approval.

3. Training and Review

All Council officers undertaking covert surveillance shall be appropriately trained to ensure that they understand their legal obligations.

This policy shall be reviewed regularly. The operation of this policy shall be overseen by the Director of Resources and Deputy Chief Executive.

4. Contact

All citizens will reap the benefits of this policy, through effective enforcement of criminal and regulatory legislation and the protection that it provides.

Adherence to this policy will minimise intrusion into citizens' lives and will avoid any legal challenge to the Council's covert surveillance activities.

Any questions relating to this policy should be addressed to the RIPA Co-ordinator Santokh Gill on 704 6006. sgill@solihull.gov.uk

The Director of Resources and Deputy Chief Executive, Paul Johnson is the Designated Senior Responsible Officer (SRO) to exercise the responsibilities under para. 4.41 of the Covert Surveillance code. who is responsible for:

- the integrity of the process in place within the public authority to authorise directed and intrusive surveillance and interference with property or wireless telegraphy;
  • compliance with Part II of the 2000 Act, Part III of the 1997 Act, section 5 of the 1994 Act and with this code;
  • oversight of the reporting of errors to the Investigatory Powers Commissioner and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;
  • engagement with the Investigatory Powers Commissioner and inspectors who support the Commissioner when they conduct their inspections;
  • where necessary, overseeing the implementation of any post-inspection action plans recommended or approved by a Judicial Commissioner, and
  • ensuring that all authorising officers are of an appropriate standard, addressing any recommendations and concerns in the inspection reports prepared by the Investigatory Powers Commissioner.

5. Magistrates' Approval

The Protection of Freedoms Act 2012 Chapter 2 of Part 2 of the 2012 Act (sections 37 and 38) requires local authorities to obtain the approval of a Magistrate for the use of any one of the three covert investigatory techniques available to them under RIPA namely Directed Surveillance, the deployment of a Covert Human Intelligence Source (CHIS) and accessing communications data. An approval is also required if an authorisation to use such techniques is being renewed. In each case, the role of the Magistrate is to ensure that the correct procedures have been followed and the relevant factors have been taken account of. The provisions allow the Magistrate, on refusing an approval of an authorisation, to quash that authorisation.

Section 38 of the 2012 Act makes provision for Magistrates' approval of local authority authorisations for the use of Directed Surveillance and the deployment of a CHIS. It does this by adding a new section 32A to Part 2 of RIPA.

Directed Surveillance is often conducted, amongst other things, to investigate a benefit fraud or to collect evidence of rogue trading/fly tipping etc. Typical methods include covertly following people, covertly taking photographs of them and using hidden cameras to record their movements. A typical example of a CHIS, is an informant using his relationship with his employer to regularly disclose information about benefit fraudsters working in a factory.

The internal authorisation for such surveillance methods is not to take effect until such time (if any) as a Magistrate has made an order approving it . Approval can only be given if the Magistrate is satisfied that:

a) There were reasonable grounds for the authorising officer approving the application to believe that the Directed Surveillance or deployment of a CHIS was necessary and proportionate and that there remain reasonable grounds for believing so.

b) The authorising officer will be of the correct seniority within the Council i.e. Head of Service/Service Manager or equivalent as per the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 (SI 2010/521) ("the 2010 Order").

The granting of the authorisation was for the prescribed purpose, as set out in the 2010 Order i.e. preventing or detecting crime (and satisfies the Serious Offence Test for Directed Surveillance (see below))

In addition to the above, where the authorisation is for the deployment of a CHIS, the Magistrate must be satisfied that:

The provisions of section 29(5) have been complied with. This requires us to ensure that there are officers in place to carry out roles relating to the handling and management of the CHIS as well as the keeping of records (as per the Regulation of Investigatory Powers (Source Records) Regulations 2000 (SI 2000/2725)).

Where the CHIS is under 16 or 18 years of age, the requirements of the Regulation of Investigatory Powers (Juveniles) Order 2000 (SI 2000/2793) have been satisfied. This sets out rules about parental consent, meetings, risk assessments and the duration of the authorisation. Note that the authorisation of such persons to act as a CHIS must come from the Chief Executive.

Where the application is for the renewal of a CHIS authorisation, a review has been carried out by the local authority and the Magistrate has considered the results of the review.

The deployment of a CHIS has to be necessary 'for the purpose of preventing or detecting crime or of preventing disorder'.

The authorising officer is not required to apply in person and there is no need to give notice to either the subject of the authorisation or their legal representatives (Section 32B(2)). This reflects the covert nature of the exercise of the investigatory powers under RIPA.

6. Directed Surveillance and the Serious Crime Test

Where RIPA is used to authorise Directed Surveillance, this should be confined to cases where the offence under investigation is a serious offence.

Directed Surveillance cannot be authorised unless it is for the purpose of preventing or detecting a criminal offence and it meets the condition set out in Article 7A(3)(a) or (b) of the 2010 Order. Those conditions are that the criminal offence which is sought to be prevented or detected is punishable, whether on summary conviction or on indictment, by a maximum term of at least 6 months of imprisonment, or would constitute an offence under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933. The latter are all offences involving sale of tobacco and alcohol to underage children.

7. 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 in preventing or detecting crime or carrying out other statutory functions, as well as in understanding and engaging with the public.

It is important that we are able to make full and lawful use of this information for 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 codes of practice from paragraphs deal with online covert activity. They are intended to us 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.

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 when 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. See also paragraph 3.6.of the code.

Example 1: A police officer undertakes a simple internet search 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, it 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: A customs 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: A public authority 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 of 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.

A member of a public authority should not adopt the identity of a person known, or likely to be known, to the subject of interest or users of the site without authorisation, and without the consent of the person whose identity is used, and without considering the protection of that person. The consent must be explicit (i.e. the person from whom consent is sought must agree (preferably in writing) what is and is not to be done).

8. CHIS (Covert Human Intelligence Source)

A **CHIS** is someone who establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything either he covertly uses such a relationship to obtain information or provide access to any information to another or he covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

When an informant gives repeat information about a suspect or about a family, and it becomes apparent that the informant may be obtaining this information in the course of a family or neighbourhood relationship, alarm bells should ring. It may mean that the informant is in reality a CHIS, who may be at risk of reprisals and to whom a duty of care is owed if the information is used. If any doubt arises, legal advice should be sought immediately.

Establishing, maintaining, and using a relationship

The word "establishes" when applied to a relationship means "set up". It does not require, as "maintains" does, endurance over any particular period. Consequently, a relationship of seller and buyer may be deemed to exist between a shopkeeper and a customer even if only a single transaction takes place. Repetition is not always necessary to give rise to a relationship, but whether or not a relationship exists depends on all the circumstances including the length of time of the contact between seller and buyer and the nature of that contact.

Example 1: Intelligence suggests that a local shopkeeper is openly selling alcohol to underage customers, without any questions being asked. A child is engaged and trained by a public authority to make a purchase of alcohol. On the basis that the exchange between a buyer and seller will be simply transactional, it is unlikely a relationship would be formed in these circumstances, and therefore it is unlikely that the child would be considered a CHIS according to the definition in Section 26(8) of the 2000 Act. A CHIS authorisation would not therefore be appropriate. However, if the test purchaser is wearing recording equipment but is not authorised as a CHIS, consideration should be given to granting a directed surveillance authorisation if it is likely to result in the obtaining of private information.

Example 2: In similar circumstances, intelligence suggests that a shopkeeper will sell alcohol to children from a room at the back of the shop, providing they have first got to know and trust them. As a consequence, the public authority decides to deploy its operative on a number of occasions, to befriend the shopkeeper and gain their trust, in order to purchase alcohol and pass back information to the public authority on the shopkeeper's activities. In these circumstances a relationship has been established and maintained for a covert purpose and therefore a CHIS authorisation should be obtained. Legend building

When a Relevant Source is deployed to establish their "legend"/ build up their cover profile, a CHIS authorisation should be considered if the activity will interfere with an individual's Article 8 rights. This will include circumstances where it is not clear to the individual with whom the source establishes or maintains a relationship that the Relevant Source is not who he or she claims to be. Interference with any individual's Article 8 rights may require a CHIS authorisation, irrespective of whether that individual is the subject of a current or future investigation. Where a CHIS authorisation is not considered necessary, arrangements should be in place to maintain active review of this position, and any decision not to authorise should be made by the person prescribed to act as the Authorising Officer.

Human source activity falling outside CHIS definition

Not all human source activity will meet the definition of a CHIS. For example, a source may be a public volunteer or someone who discloses information out of professional or statutory duty, or who has been tasked to obtain information other than by way of a covert relationship. Further detail on each of these circumstances is provided below.

Public volunteers

In many cases involving human sources, the source will not have established or maintained a relationship for a covert purpose. Many sources provide information that they have observed or acquired other than through a relationship. This means that the source is not a CHIS for the purposes of the 2000 Act and no CHIS authorisation is required.

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

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

Professional or statutory duty

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

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

Tasking not involving relationships

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

Example: A member of the public is asked by a member of a public authority to maintain a record of all vehicles arriving and leaving a specific location or to record the details of visitors to a neighbouring house. A relationship has not been established or maintained in order to gather the information and a CHIS authorisation is therefore not available. Other authorisations under the 2000 Act, for example, a directed surveillance authorisation, may need to be considered where the activity is likely to result in the public authority obtaining

information relating to a person's private or family life. Identifying when a human source becomes a CHIS

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

Determining the status of an individual or organisation is a matter of judgement by the public authority. Public authorities should avoid inducing individuals to engage in the conduct of a CHIS, either expressly or implicitly, without obtaining a CHIS authorisation or considering whether it would be appropriate to do so. 12

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

9. **Responsibility for RIPA matters**

A lead officer (a Solicitor in Legal Services) (referred to in this procedure as the "RIPA co-ordinator) is responsible for the maintenance of the centrally retrievable record of authorisations, renewals, reviews and cancellations giving day to day advice on the application of RIPA to Council Officers and the implementation of officer training.

Documents sent to the RIPA Co-ordinator must be addressed:-
The Solicitor to the Council FAO (RIPA Co-ordinator), Legal Services, Council House, Solihull B91 3QS).or emailed sgill@solihull.gov.uk

The Director of Resources and Deputy Chief Executive is the Designated Senior Responsible Officer (SRO) to exercise the responsibilities under para. 3.29 of the Covert Surveillance code.

In terms of monitoring e-mails and internet usage, it is important to recognise the important interplay and overlaps with the Council's e-mail and Internet policies and guidance, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, the Data Protection Act 1998 and its Codes of Practice. .

RIPA authorises local authorities to carry out directed covert surveillance and also the use or conduct of a covert use of a human intelligence source. Proper use of RIPA will be to make lawful any conduct authorised and carried out in accordance with it and evidence admissible in court.

The Human Rights Act 1998 requires the Council under Article 8 of the European Convention to respect the private and family life of citizens, his home and his correspondence. The European Convention did not however make this an absolute right but a qualified right. Accordingly, in certain circumstances, the Council may interfere in the citizen's right mentioned above, if such interference is
in accordance with the law necessary and proportionate

RIPA provides a statutory mechanism for authorising covert surveillance and the use of a covert human intelligence source (CHIS). It also permits Public Authorities to compel telecommunications and postal companies to obtain and release communications data. 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. A consequence of not following RIPA is that a person's human rights could be breached and could render the Council liable to a claim for damages under the Human Rights Act 1998

A consequence of not complying with RIPA is that a complaint may be made to the Tribunal set up under RIPA which has wide powers to make orders and award compensation. Any evidence obtained by covert surveillance without a RIPA authority may be inadmissible in court.

Surveillance includes monitoring, observing, listening to persons, watching or following their movements, listening to their conversations and other such activities or communications, recording anything mentioned above in the course of authorised surveillance. Surveillance, can be via or with, the assistance of appropriate surveillance device(s). It can be overt or covert.

10. Necessity and proportionality

Obtaining an authorisation under RIPA will ensure that there is a justifiable interference with an individual's Article 8 rights if it is necessary and proportionate for these activities to take place. The 2000 Act requires that the person granting an authorisation believes that the authorisation is necessary in the circumstances of the particular case.

The Council cannot authorise Directed Surveillance unless it is for the purpose of preventing or detecting a criminal offence and it meets the condition set out in Article 7A(3)a or (b) of the 2010 Order. The criminal offence which is sought to be prevented or detected is punishable by a maximum term of at least 6 months imprisonment or would constitute an offence under section 146, 147, 147A of the Licensing Act 2003 or Section 7 Childrens and Young Persons Act 1933.

If the activities are necessary, the person granting the authorisation must believe that they are proportionate to what is sought to be achieved by carrying them out. This involves balancing the intrusiveness of the activity on the target and others who might be affected by it against the need for the activity in operational terms. The activity will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means. All such activity should be carefully managed to meet the objective in question and must not be arbitrary or unfair.

Officers must carefully consider the likelihood of collateral intrusion occurring. This is the risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation. If the risk is significant, measures should be taken to avoid, where possible, any unnecessary intrusion. For e.g. considering changing timing of surveillance, amount, method and sensitivities of the local community.

Proportionality therefore contains four concepts:
a) balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence,
b) Explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others,
c) Considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives,
d) Evidencing as far as reasonably practicable what other methods had been considered and why they were not implemented..

11. The need for authorisations

Authorisation will ensure that covert surveillance and the use or conduct of a covert human intelligence source will be lawful and evidence obtained will be admissible in legal proceedings.

All authorisations must only be given following an application by the Investigating Officer made on the appropriate form. The Council's Authorising Officers – Steve Sparkes Head of Audit and Alison McGrory Assistant Director for Stronger Communities, Economy and Infrastructure.
Authority for covert surveillance and the use or conduct of a covert human intelligence source may only be given by an officer who has been specifically designated and approved by the Chief Executive/Director of Resources and Deputy Chief Executive.

Authorisation for RIPA must be given personally by the Authorising Officer. This responsibility cannot be delegated. (See Para. 4.11 of the Covert Surveillance Code of Practice).

Special rules apply under RIPA where the use or conduct of a covert human intelligence source may lead to the acquisition of confidential information or where a juvenile or vulnerable person is to be used as a source. RIPA requires that in these cases authorisation can only be given by the Chief Executive or in his absence a chief officer.

Authorising Officers must receive training or briefing arranged by the RIPA Co-ordinator before considering the grant of any authorisation. It will be the responsibility of Authorising Officers to ensure that their relevant members of staff are suitably trained as 'Applicants' so as to avoid common mistakes appearing on the RIPA forms.

A written authorisation granted by an authorising officer will cease to have effect (unless renewed or cancelled) at the end of a period of three months (or six months for intelligence services' authorisations) beginning with the day when the authorisation granted had taken effect.

12. Duties of Authorising Officers

Authorisation of covert surveillance must not be granted as a matter of formality without proper inquiry and consideration of all the circumstances. Authorising officers must be familiar with the any RIPA changes and/or consult the RIPA co-ordinator.

The Authorising Officer must ensure that the authorisation sought is permitted by RIPA and that the application forms are properly completed by the officer requesting authorisation. Any cases of doubt must be referred to Legal Services for advice.

As mentioned above, RIPA sets out the grounds under which authorisation is required for directed surveillance and for Covert Human Intelligence Source (CHIS). The Authorising Officer must consider whether the grant of authorisation for directed surveillance and/or CHIS will constitute an interference with a person's rights under the European Convention on Human Rights, in particular Article 8 which relates to the respect for private and family life.).

The authorising Officer must be satisfied that the RIPA authorisation is in accordance with the law, necessary in the circumstances of the particular case and is proportionate.

In assessing whether or not the proposed surveillance is proportionate, consider whether there are any other non-intrusive methods, and if there are none, whether the proposed surveillance is no more than necessary to achieve the objective, as the least intrusive method will be considered proportionate by the courts.

The Authorising Officer must ensure that the authorisation will not involve intrusive surveillance which RIPA does not allow a local authority officer to authorise.

The Authorising Officer must before granting an authorisation consider the risk of collateral intrusion into the privacy of persons who are not connected with the investigation or operation and whether steps are needed to minimise this. The authorising forms must contain details of this consideration.

The Authorising Officer must consider whether the proposed directed surveillance is justified, proportionate and necessary to what it seeks to achieve.

The Authorising Officer must insert adequate reasons to justify necessity and proportionality. Consideration of the issue of proportionality requires the Authorising Officer to consider

whether the surveillance proposed is an appropriate measure to obtain evidence, bearing in mind the seriousness of the particular matter being investigated.

If the authorisation is refused, the Authorising Officer must ensure that the Investigating Officer making the application is clearly aware of the refusal and its implications. The fact of refusal must be clearly endorsed.

A copy of the completed application form (refused or granted) must be passed to the Investigating Officer making the application and the original form must be sent to the RIPA Co-ordinator within a week of the authorisation/refusal.

The Authorising Officer must keep under review all authorisations given by him and retain any records of reviews of the authorisation. Each RIPA authority/review/cancellation must be sent/emailed to the RIPA co-ordinator.

Where the Authorising Officer decides to cancel the authorisation, the cancellation form must be sent to the Investigating Officer and the RIPA Co-ordinator at the address in paragraph 2.4 above within a week of the cancellation.

Although an authorisation for directed surveillance will have effect for a period of 3 months after it takes effect, it must if it is to continue, be renewed by the Authorising Officer following an application made by the Investigating Officer. If an authorisation is not to be renewed, it must be cancelled promptly and not just allowed to lapse.
A copy of the completed renewal application form must be passed to the Investigating Officer and a copy to the RIPA Co-ordinator The authorising officer shall then consult the RIPA Co-ordinator to arrange judicial approval.

If the Authorising Officer is directly involved in an investigation himself and there is no other officer available to give authority, the fact that he is directly involved must be noted on the forms.

Authorising Officers must pay particular attention to Health and Safety issues that may be raised by any proposed surveillance activity. Under no circumstances, should an Authorising Officer approve any RIPA form unless, and until he/she are satisfied that the health and safety of Council employees/agents are suitably addressed and/or risks minimised, so far as is possible, and proportionate to/with the surveillance being proposed. If in any doubt guidance should be sought from the Council's Health and Safety Officer and/or the RIPA co-ordinator.

Authorising Officers must consider coming across Confidential Information during surveillance and must give it prior thought before approving any RIPA forms. When authorising the conduct or use of a CHIS, the Authorising Officer must also –

Be satisfied that the conduct and/or use of the CHIS is proportionate to what is sought to be achieved;

Be satisfied that appropriate arrangements are in place for the management and oversight of the CHIS and this must address health and safety issues through a risk management;

Consider the likely degree of intrusion of all those potentially affected;

Consider any adverse impact on community confidence that may result from the use or conduct of the information obtained;

Ensure records contain particulars and are not available except on a need to know basis; and

If unsure on any matter to obtain advice from the RIPA co-ordinator before signing any forms.

Particular considerations apply where the Authorising Officer is requested to authorise the use or conduct of a CHIS source where Confidential information (matters subject to legal privilege, confidential personal information or confidential journalistic information) is likely to be acquired.

Particular considerations also apply where Vulnerable individuals (including persons who are receiving or may need community care services and are unable to protect themselves from harm or exploitation) are to be used as a source; or Juveniles (persons under 18) are to be used as a source
In any of these cases a higher level of approval will be required from the Chief Executive or in his absence a chief officer. Special rules1 apply to the use of juveniles as a covert human intelligence source and these are set out in Appendix 5.
If the application is approved (and any higher approvals required are given) the Authorising Officer must send to the Investigating Officer making the application a copy of the form and send the original form to the RIPA Co-ordinator within a week of authorisation.

Applications should be in writing (unless urgent) and should describe the conduct to be authorised and the purpose of the investigation or operation. The application should specify:

<u>Information to be provided in all applications</u>

• the reasons why the authorisation is necessary in the particular case and on which statutory ground(s) (e.g. for the purpose of preventing or detecting serious crime) listed in section 32(3) and 32(3A)53 of the 2000 Act;
• the nature of the surveillance;
• the residential premises or private vehicle in relation to which the surveillance will take place, where known;
• the identities, where known, of those to be the subject of the surveillance;
• an explanation of the information which it is desired to obtain as a result of the surveillance;
• details of any potential collateral intrusion and why the intrusion is justified;
• details of any confidential or privileged information that is likely to be obtained as a consequence of the surveillance;

13. Duties of the Investigating Officer

The Investigating Officer shall before making an application for any surveillance consider the evidence which is to be obtained and whether it is necessary, lawful and proportionate to acquire evidence by covert surveillance. If in doubt the Investigating Officer should seek advice from the RIPA Co-ordinator in Legal Services.
The Investigating Officer shall consider, before making an application, whether a risk assessment is necessary and shall not unless the matter is urgent (in which case it shall be dealt with under the urgent procedure) undertake any covert surveillance until such surveillance has been authorised.

The Investigating Officer shall complete the relevant parts of the RIPA forms and submit them to his Authorising Officer and should be familiarise themselves with the paragraphs above on the role of what the authorising officer will consider before approving any RIPA forms. Once obtaining authorisation, the investigating officer must liaise with the RIPA Co-ordinator or legal services on arranging a court hearing. The investigating officer will then be authorised under S223 Local Government Misc Provisions Act 1972 or a solicitor will attend court with the officer. Once judicial approval has been given a copy of the authority must be given/emailed to the Authorising Officer and to the RIPA Co-ordinator.

The Investigating Officer shall retain all evidence arising from directed surveillance in accordance with the rules for retention and disclosure under the Criminal Procedure and Investigations Act 1996.

The Investigating Officer shall retain copies of all RIPA notices issued to him by the Authorising Officer and give details of such notices in his report recommending the consideration of legal proceedings or other action to be taken by the Council.

The Investigating Officer requesting a CHIS must carry out a risk assessment before making an application for the use or conduct of a covert human intelligence source to determine the risk to the source and of any tasking and the likely consequences should the role of the source become known. The risk assessment, which must be recorded in writing, must also consider the security and welfare of the source after an authorisation is cancelled.

14. Central Record of Authorisations

The RIPA Co-ordinator shall keep the centrally retrievable indexed record of authorisations, renewals, reviews and cancellations for directed surveillance and the use or conduct of a covert human intelligence source together with copies of the completed RIPA forms including the cancellation forms.

The record and forms shall be kept securely as a private and confidential document.
Only Authorising Officers and other persons entitled by law shall have access to the record and forms.

Records will be available for inspection by the Investigatory Powers Commissioner and retained for 3 years from cancellation to allow the Investigatory Powers Tribunal ('IPT'), established under Part IV of the 2000 Act, to carry out its functions.

15. Safeguarding Material obtained through covert surveillance or property interference

May only be copied to the extent necessary for the authorised purposes. Copies include not only direct copies of the whole of the material, but also extracts and summaries which identify themselves as the product of covert surveillance or property interference, and any record which refers to the covert surveillance or property interference and the identities of the persons to whom the material relates.

Material obtained through covert surveillance or property interference, and all copies, extracts and summaries of it, must be handled and stored securely, so as to minimise the risk of loss or theft. It must be held so as to be inaccessible to persons without the required level of security clearance (where applicable). This requirement to store such material securely applies to all those who are responsible for the handling of the material.

In particular, officers must apply the following protective security measures:

• physical security to protect any premises where the information may be stored or accessed;
• IT security to minimise the risk of unauthorised access to IT systems;
• an appropriate security clearance regime for personnel which is designed to provide assurance that those who have access to this material are reliable and trustworthy.

Destruction

Information obtained through covert surveillance or property interference, and all copies, extracts and summaries which contain such material, should be scheduled for deletion or destruction and securely destroyed as soon as they are no longer needed for the authorised purpose(s). If such information is retained, it should be reviewed at appropriate intervals to confirm that the justification for its retention is still valid. In this context, destroying material means taking such steps as might be necessary to make access to the data impossible.

16. Errors

An error must be reported if it is a "relevant error". Under section 231(9) of the 2016 Act, a relevant error for the purpose of activity covered by this code is any error by the council in not complying with any requirements that are imposed on it by any enactment which are subject to review by a Judicial Commissioner. This would include compliance with Part II of the 2000 Act Examples of relevant errors occurring would include circumstances where:

-Surveillance or property interference activity has taken place without lawful authorisation.

-There has been a failure to adhere to the safeguards set out in the relevant statutory provisions of the Guidance. Errors can have very significant consequences on an affected individual's rights and, in accordance with section 235(6) of the 2016 Act, all relevant errors made by public authorities must be reported to the Investigatory Powers Commissioner by the council once aware of the error.

When a relevant error has occurred, and the council made aware, the Investigatory Powers Commissioner (IPC) must be notified as soon as reasonably practicable, and no later than ten working days (or as agreed with the Commissioner) after it has been established by appropriate internal governance processes that a relevant error has occurred as stated in paragraphs 8.8 to 8.18 of the Guidance.

A full report must be sent to the IPC as soon as reasonably practicable in relation to any relevant error, including details of the error and, where it has not been possible to provide the full report within ten working days (or as agreed with the Commissioner) of establishing the fact of the error, the reasons this is the case. The report should include information on the cause of the error; the amount of surveillance or property interference conducted and material obtained or disclosed; any unintended collateral intrusion; any analysis or action taken; whether any material has been retained or destroyed; and a summary of the steps taken to prevent recurrence.

The IPC may issue guidance as necessary, including guidance on the format of error reports. In addition to the above, errors may arise where a warrant or authorisation has been obtained and as a result having been provided with information which later proved to be incorrect due to an error on the part of the person providing the information, but on which the council relied in good faith. Whilst these actions do not constitute a relevant error on the part of the authority which acted on

• Surveillance or property interference activity has taken place without lawful authorisation.
• There has been a failure to adhere to the safeguards set out in the relevant statutory provisions and Chapter 9 of the Code of Practice.

Serious Errors

Section 231 of the 2016 Act states that the Investigatory Powers Commissioner must inform a person of any relevant error relating to that person if the Commissioner considers that the error is a serious error and that it is in the public interest for the person concerned to be informed of the error. The Commissioner may not decide that an error is a serious error unless he or she considers that the error has caused significant prejudice or harm to the person concerned. The fact that there has been a breach of a person's Convention rights (within the meaning of the Human Rights Act 1998) is not sufficient by itself for an error to be a serious error.

In deciding whether it is in the public interest for the person concerned to be informed of the error, the Commissioner must in particular consider:

national security;

the prevention or detection of serious crime;
the economic well-being of the United Kingdom; or
the continued discharge of the functions of any of the intelligence services.

Before making his or her decision, the Commissioner must ask the council to make submissions on the matters concerned. Public authorities must take all such steps as notified to them by the Investigatory Powers Commissioner to help identify the subject of a serious error.

When informing a person of a serious error, the Commissioner must inform the person of any rights that the person may have to apply to the Investigatory Powers Tribunal, and provide such details of the error as the Commissioner considers to be necessary for the exercise of those rights.

17. Use of CCTV

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

- wish to use the Council's resources (e.g. CCTV surveillance systems), 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, s/he must obtain a copy of that agency's RIPA form for the record (a copy of which must be passed to the RIPA co-ordinator) or relevant extracts from the same which are sufficient for the purposes of protecting the Council and the use of its resources;

- wish to use the Council's premises for their own RIPA action, and is expressly seeking assistance from the Council, 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. Suitable insurance or other appropriate indemnities may be sought, if necessary, from the other agency for the Council's co-operation in the agent's RIPA operation. In such cases, however, the Council's own RIPA forms should not be used as the Council is only 'assisting' not being 'involved' in the RIPA activity of the external agency.

If the Police or other Agency wish to use Council resources for general surveillance, as opposed to specific RIPA operations, an appropriate letter requesting the proposed use, extent of remit, duration, 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.

If in doubt, please consult with the RIPA co-ordinator at the earliest opportunity.

18. Independent Oversight

RIPA was originally overseen by the Office of Surveillance Commissioners (OSC). From 1 Sept 2017 oversight for both RIPA and IPA is now provided by the Investigatory Powers Commissioner's Office (IPCO). IPCO is the independent inspection office whose remit

includes providing comprehensive oversight of the use of the powers to which RIPA, IPA and the Codes apply, and adherence to the practices and processes described therein.

They also provide guidance to be followed which is separate to the Codes. Regulation of Investigatory Powers Policy and Guidance

IPCO has unfettered access to all locations, documentation and information systems as is necessary to carry out its full functions and duties and will periodically inspect the records and procedures of the Council to ensure the appropriate authorisations have been given, reviewed, cancelled, and recorded properly.

It is the duty of any person who used investigatory powers to comply with any request made by a Commissioner/Inspector to disclose or provide any information they require for the purpose of enabling them to carry out their functions. is, therefore, important that the Council can show it complies with this Policy and with the provisions of RIPA.

November 2022