TAMESIDE METROPOLITAN BOROUGH COUNCIL

POLICY AND
PROCEDURAL GUIDE

To be read in conjunction with the Covert Surveillance and Property interference Revised Code of Practice and the Covert Human Intelligence Sources Revised Code of Practice August 2018

Revised October 2022

FOR THE USE OF COVERT SURVEILLANCE
AND
COVERT HUMAN INTELLIGENCE SOURCES ("CHIS")

To comply with the Regulation of Investigatory Powers Act 2000, all its Regulations, the Human Rights Act 1998 and having regard to the Codes of Practice published by the Secretary of State under S71(3)(a) of the Regulation of Investigatory Powers Act 2000

INDEX

Heading			Page No.
A	**GENERAL INTRODUCTION**		**1**
B	**DEFINITIONS**		**3**
1.	Authorisation		**3**
2.	Authorising Officer		**4**
3	Covert		**4**
4	Confidential Material		**5**
5	Covert Human Intelligence Source (CHIS)		**6**
6	Directed Surveillance		**6**
7	Intrusive Surveillance		**6**
8	Necessary		**7**
9	Private Information		**7**
10	Private Vehicle		**7**
11	Proportionate		**8**
12	Residential Premises		**8**
13	Subjects		**9**
14	Surveillance		**9**
15	Surveillance Device		**9**
16	Urgent authorisations		**9**
C	**AUTHORISATIONS**		
1	Application		**9**
2	Written Authorisations		**10**
3	Requirements		**10**
4	Authorising Officer Process		**10**
5	Officers Roles & Procedure		**11**
6	Urgent RIPA applications		**12**
7	Information to be included in the application		**14**
8	Obtaining Judicial Authorisation		**15**
9	Additional Subjects/Targets		**15**
10	Covert Human Intelligence Sources (CHISs)		**16**
11	Covert Human Intelligence Sources: Criminal Conduct Authorisation Process		**16**
12	Records Relating to the CHIS		**17**
13	Reviews		**19**
14	Renewals		**19**
15	Cancellation		**19**
16	Errors		**19**
D	**RECORDS**		**20**
E	**EQUIPMENT**		**26**
F	**CIVIL LIBERTY**		**26**
G.	**COMPLAINTS**		**26**

H FORMS 26

I THE APPLICATION AND AUTHORISATION FORMS (INCLUDING REFUSALS) 27

J PRACTICAL EXAMPLES, GUIDANCE AND ADVICE IN SPECIFIED CIRCUMSTANCES 29

K PROCESS MAPS.....39

A. GENERAL INTRODUCTION

This Policy along with the statutory Codes of Practice published by the Secretary of State, revised in August 2018 and the Office of Surveillance Commissioners Procedures and Guidance must be readily available at Tameside Metropolitan Borough Council, Civic Centre (hereinafter referred to as the Council) for consultation and reference by Investigating Officers, Members of the Council and the public and/or their representatives.

The Policy may be amended from time to time by the Executive Director Governance and Resources, to reflect the most up to date and relevant guidance, and will be kept under review by the Council's Enforcement Coordination Panel and as directed by the Executive Director Governance and Resources.

If the Council receives an FOI request for an IPCO inspection report of our organisation, this should be brought to the attention of IPCO's Data Protection Officer at info@ipco.org.uk before making any disclosures.

If we wish to publish an IPCO Inspection Report, please note that the Council must first contact IPCO's data protection officer at info@ipco.org.uk.

These documents can be obtained from and as directed by the Executive Director – Governance and Resources Tameside One, Market Place, Ashton-Under-Lyne sandra.stewart@tameside.gov.uk.

1. This Policy applies to **any** covert surveillance or use of CHISs by Council employees whose duties include investigation under properly delegated powers and by private investigators engaged to act as agents by those employees. It should be emphasised that RIPA will only apply if the surveillance or use of CHIS is **'covert'**; quite often such activities will be done overtly and so will fall outside RIPA 2000 so it is advisable to be familiar with the definition of 'covert' under RIPA as a starting point. **A local authority may only use covert surveillance for the purpose of the prevention or detection of crime the offence of which must attract a custodial sentence of six months or more or criminal offences relating to the underage sale of tobacco or alcohol**.

2. This Policy has been drafted specifically for Tameside Council and has regard to the provisions of the Codes of Practice issued by the Secretary of State under S71 RIPA 2000. It should be noted that S72(1) RIPA states that a person exercising or performing any power or duty in relation to which provision may be made by a code of practice under Section 71 shall, in doing so, have regard to the provisions (so far as they are applicable) of every code of practice for the time being in force under that section. This Policy has been compiled especially for the Council only omitting elements which are not applicable to the Council. For example, there is no power of authorisation for **'intrusive surveillance'** (see definition B6 in the Code) so references to such authorisations have been omitted.

3. **All** covert surveillance or use of CHIS's should be authorised in writing and in accordance with this Policy and should only be authorised if it is necessary for the purpose of preventing or detecting crime or of preventing disorder. It should then be carried out in accordance with the authorisation.

4. In addition, covert surveillance and the use of CHISs should only be used by the Council where the Authorising Officer believes it is **"proportionate"** (see definitions section below).

5. **Before** authorising covert surveillance properly appointed **Authorising Officer** should also take into account the risk of intrusion into the privacy of persons other than the specified subject of the surveillance (collateral intrusion) and take measures wherever practicable to avoid it. Similarly they should also be aware of the possibility (though rare) of obtaining confidential information and take measures to avoid it.

6. As far as surveillance is concerned this Policy is only concerned with '**directed'** surveillance (see definitions below). This authority must not carry out 'intrusive surveillance' unless the Police are involved and the surveillance is conducted by them in accordance with their authorisation procedure. In cases of joint investigations with the Police, SOCA or CTU no covert activities should take place **unless** the Council is satisfied that the Police, SOCA or CTU have obtained their own authorisation under RIPA. In order to be 'satisfied, the Council's **Senior Authorising Officer** should be allowed to have sight of the particular RIPA authorisation and ensure that a written record has been made on the Council's file that such authorisation has been checked. The purpose of this procedure is to safeguard the Council against potential claims by persons who allege their actions are unlawful or without authorisation. Should such authorisation not be available for inspection the Council shall not continue with any covert activities without its own RIPA authorisation.

7. There should be no situation in which an **Investigating Officer** has to engage in covert surveillance or using aCHIS without obtaining authorisation. **However,** it should be noted that Section 80 of the Act provides that without an authorisation the actions of the public authority would **not** be made unlawful by RIPA. Nonetheless, such unauthorised covert surveillance or use of a CHIS could contravene **Article 8** European Convention of Human Rights (the right to respect for one's private and family life) brought into force in the UK by the Human Rights Act 1998. Evidence obtained by covert means could also be challenged in court for a breach of **Article 6** of the European Convention on Human Rights (right to a fair trial) on the grounds that it was unlawfully obtained, thus jeopardising a criminal prosecution with potentially expensive and reputationally damaging consequences., Having an authorisation therefore makes it less likely that the covert surveillance or use of CHIS could be held to breach the Human Rights Act 1998, or be challenged in the Courts because it then becomes **"lawful for all purposes"** (Section 27(1) RIPA 2000).

8. For the avoidance of doubt, surveillance notified to the subject is **not** covert and so does not fall within the provisions of RIPA. The same applies if information is obtained in an **overt** way, for example, when an officer behaves as an ordinary member of the public making test purchases or when checks are made on labelling etc which can only be made when overtly looking or asking questions. Such actions are often already authorised specifically by other legislation in any event.

9. In addition common-sense of course dictates that no surveillance will be undertaken from a property e.g one situated next door or nearby the subject's property, **unless** the person who occupies the premises from which the surveillance is to take place has been notified and their consent obtained.

10. Where an Authorising Officer receives an application for covert surveillance or CHIS which he considers should not be granted, he should strike the form through with two black lines and send it to the Surveillance Monitoring Officer with a note giving reasons for refusal. This will then be logged and a record kept. It will prove useful when inspected by the office of Surveillance Commissioners to show that the quality assurance system is operating at the source.

11. It has been made clear in the Covert Surveillance and Property Interference (Revised Home Office Code of Practice August 2018) pursuant to Section 71 of RIPA that Members should not be involved in making decisions and specific authorisations. The Surveillance Monitoring Officer may want to keep members informed of the processes followed under RIPA through for example the Enforcement Co-ordination Panel, as and when they arise, and in any event, Elected Members of a local authority should review their authority's use of the 2000 Act and its policy annually.

B. DEFINITIONS

1. **Authorisation**

An authorisation is the final part of a completed R1/DS or R1/CHIS form authorising covert surveillance or use of a covert human intelligence source. It is the part of the form headed 'Authorising Officer's Section'.

Critically it must contain the Authorising Officer's view of **why** the activity is necessary for the prevention or detection of crime or disorder and why it is proportionate. It also contains the details of what the Authorising Officer actually wants to authorise, namely how many Officers, type of activity, how they will carry it out, what equipment eg cameras, CCTV, vehicles they will use, where it is to take place and strategy such as positioning so as to avoid unnecessary intrusion.

It contains the time and date it is to commence and the time and date 3 months later (unless it is a CHIS – then it is 12 months) when it is to finish. It contains review dates, usually monthly. S/He will sign their name, rank and date.

There is also provision for the Head of Paid Service/Chief Executive to authorise if there is a risk of obtaining confidential information, and an explanation of how it will assist the investigation.

The Protection of Freedoms Act 2012 introduced an additional stage in the process. **After** the form has been countersigned the local authority must seek judicial approval for the RIPA Authority.

A Justice of the Peace will decide whether a local authority grant or renewal of an authority or notice to use RIPA should be approved and it will not come into effect unless and **until** it is approved by a JP.

The officer must complete forms for judicial approval which can be found at RIPA Home Office Guidance for Magistrates Court. Copies of the forms are also kept within the Central Record retained in Legal Services. These forms must not be amended and applications will not be accepted if the approved forms are not completed. https://www.gov.uk/government/collections/ripa-forms--2

The forms must be submitted with the authorisation to the Head of Legal Services and a suitable date and time for an application for judicial approval will be made. Authorisations are also subject to judicial approval.

2. Authorising Officer

2.1 This can be 'a Director, Head of Service, Service Manager or Equivalent' (see Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 SI No 521 in force on 06/04/10). Therefore for the purposes of this Policy the authorising Officer shall be an officer of one of those ranks who may be appointed by the Council's Monitoring Officer (the Executive Director of Governance and Resources) to hold the position of 'Authorising Officer'. At the moment only the Monitoring Officer and the Assistant Executive Director of Place hold this rank.

3. Covert

This is **defined** in Section 26(9)(a) of the RIPA as follows:

'Surveillance is covert if and only if it is carried out in a manner that is calculated to ensure that the persons who are subject to the surveillance are unaware that it is or may be taking place'.

Therefore, if you notify a person that they are to be monitored in a particular way, or if you put up CCTV cameras and erect public notices it is not covert and, therefore, RIPA is not engaged.

4. **Confidential Material**

This has the same meaning as is given to it in sections 98-100 of the Police Act 1997.

It consists of matters subject to legal privilege, confidential personal information, or confidential journalistic material:

Matters subject to legal privilege includes both oral and written

Communications between a professional legal adviser and his or her client or any person representing his or 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.

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

- either to his or her physical or mental health; or
- to spiritual counselling or other assistance given or to be given, and
- which a person has acquired or created in the course of any trade, business, profession or other occupation, or for the purposes of any paid or unpaid office. 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:
- it is held subject to an express or implied undertaking to hold it in confidence; or
- it is subject to a restriction of 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 purposes of journalism and held subject to such an undertaking.

NOTE: Only the Head of Paid Service has the delegated power to authorise directed surveillance or the use of a CHIS which will result in the obtaining of Confidential Material.

5. **Covert Human Intelligence Source ("CHIS")**

This is defined in S26 (8) RIPA as follows:

'...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 to provide access to any information to another person; or

(c) he covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.'

(The RIPA also says that references to the use of a CHIS include inducing asking or assessing a person to engage in the conduct of a CHIS or to obtain information by means of the conduct of a CHIS.

6. **Directed Surveillance**

This is defined in Section 26(2) of the RIPA which says surveillance is directed if it is covert but not intrusive and is undertaken:

(a) for the purposes of a specific investigation or specific operation;

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

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

Therefore, by way of a summary, it is covert surveillance which is planned in advance to further a particular investigation and which is likely to result in the obtaining of information about a person's private or family life.

7. **Intrusive Surveillance**

Section 26(3) states that intrusive surveillance is covert surveillance that:

'(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'.

However, Section 26(5) says that surveillance which

(i) is carried out by means of a surveillance device in relation to anything taking place on any residential premises or in any private vehicle; but

(ii) is carried out without that device being present on the premises or in the vehicle is NOT intrusive, **unless the device is such that it consistently provides information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the vehicle'.**

However the Local Authority have no power to authorise intrusive surveillance.

8. '**Necessary'**

In order for an Authorising Officer to decide whether an authorisation is necessary it must fall within ground (b) which is set out in Section 28 sub-section 3 of the RIPA namely :-

(b) for the purpose of preventing or detecting crime or of preventing disorder;

(c) Amendments to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010. mean that a local authority can **now only grant** an authorisation under RIPA for the use of directed surveillance where the local authority is investigating particular types of criminal offences. These are criminal offences which attract a maximum custodial sentence of six months or more **or** criminal offences relating to the underage sale of alcohol or tobacco.

9. **Private Information**

This is defined in the Act as including, 'in relation to a person', any information relating to his or her private or family life.

10. **Private Vehicle**

This is defined in the Act as any vehicle used primarily for the private purposes of the person who owns it or of a person otherwise having the right to use it (from the latter, paying passengers are excluded). From the point of view of a paying passenger therefore, the vehicle is **not** private.

11. ‘**Proportionate’**

There is no statutory definition but in order for covert surveillance or use of CHIS to be proportionate, it **must not be used** in cases where other more open methods of investigation will suffice. This is a very important concept and all relevant officers should be aware of it.

The following points should be considered:

1. Such methods must also only be used in cases where they are likely to result in the gathering of **cogent evidence** and in cases where there is dependable intelligence to support its use.

2. The subject's situation and any known history should also be taken into account and the seriousness of the offence.

3. It is about **balancing** the seriousness of the crime being investigated and the threat to the general public against the interference with the privacy of the individual concerned.

4. Interference with a person's right to privacy will **not** be justifiable if the means used to achieve the aim are excessive in all the circumstances.

5. For example, it could be justified on the ground that there may be no other way of obtaining the evidence or perhaps a short period of surveillance could be justified on the grounds that it would be a quicker and easier way of obtaining evidence.

6. The risk of **collateral intrusion** should also be considered when looking at proportionality as a high risk of this may tip the balance in favour of not using surveillance at all unless the risk can be minimised satisfactorily. One way of reducing the risk of collateral intrusion is to target particular times for the surveillance when the subject is at large and it is good practice to detail on the RI application the times in the day when the surveillance is to be carried out eg “6.30 am to 7.45 am”.

12. **Residential Premises**

Section 48 subsection (1) provides that ‘residential premises’ mean (subject to subsection (7)(b)) so much of any premises as is for the time being occupied or used by any person, however temporarily, for residential purposes or otherwise as living accommodation (including hotel or prison accommodation that is so occupied or used). RIPA states that the words ‘residential premises’ do not include a reference to so much of any premises as constitutes any common area to which the resident has access in connection with his use or occupation of any accommodation (Section 48(7)(b) RIPA). Therefore, surveillance from a

common area is technically not intrusive, but there may be a higher risk of obtaining private information about someone so this must be considered when deciding whether or not to authorise the surveillance. For example, the entrance hall, stairs and lift in a block of flats is not counted as residential premises and this is important when assessing whether surveillance is intrusive or not.

13. **Subjects**

A member of the public or group thereof in respect of whom surveillance or the use of a CHIS has been authorised and such observed contacts of that individual or group of individuals as may come to notice during the course of the authorised surveillance or the use of a CHIS.

14. **Surveillance**

This is defined in the Regulation of Investigatory Powers Act 2000 (i.e. the RIPA) as including:

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

(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.

15. '**Surveillance Device'**

This is defined in Section 48(1) of RIPA as meaning 'any apparatus designed or adapted for use in surveillance'.

This therefore includes cameras, video cameras, listening and recording devices etc.

16. **Monitoring Officer**

The Surveillance Monitoring Officer for Tameside Council is also the Council's Executive Director for Governance and Resources.

C. AUTHORISATIONS

1. **Application**

The application must be made by the Investigating Officer to the Authorising Officer (see definition B2 above) using the forms downloaded from the intranet site. Search under the words 'Regulation of Investigating Powers' to locate the site or the Home Office website.

2. **Written Authorisations** (See also definition at B1 & B2 above)

Authorisations or renewals of authorisations must be given by the Authorising Officer in writing. At the time, an authorisation is given the Authorising Officer should diary the matter for a review in a month's time. The only Officer officially able to authorise surveillance or CHIS where confidential material is likely to be obtained is the Executive Director of Governance and Resources.

Amendments in the Protection of Freedoms Act 2012 mean that local authority authorisations can only be given effect once an Order approving the authorisation or notice has been granted by a Justice of the Peace (JP).

3. **Requirements**

Before giving authorisation for surveillance or the use of a CHIS the **Authorising Officer** must be satisfied that:

(a) it is **necessary** for the purpose of preventing or detecting crime or of preventing disorder (see definition 8 above). (You must specify the crime being investigated.)

(b) it is **necessary** in that particular case, i.e. that particular case merits the use of this method of detection over other less underhand methods eg if it is a case where a person is suspected of having committed a crime like theft, justify why is this covert method of detection is necessary to obtain the evidence over other methods

(c) it is **proportionate** (see definition 11 above) to the seriousness of the crime or the matter being investigated and the history and character of the subject concerned. Balance the likelihood of obtaining private information against the seriousness of the crime being investigated.

(d) For (a) (b) and (c) the Authorising Officer must be satisfied that there is sufficient intelligence about the suspect and the alleged offence to justify the authorisation.

4. **Authorising Officer Process**

a. In order to appoint an authorising officer, an application must be made in writing to the Surveillance Monitoring Officer and Borough Solicitor.

b. Only those who can demonstrate that they have received the appropriate training and/or had operational experience in the use of the procedures during the course of their employment shall be eligible. After proper appointment, the name shall be placed upon a Flow Chart on the

Council's intranet site and that shall be evidence of the appointment having taken place. At the moment that is not necessary.

c. In order to ensure that an Authorising Officer is equipped with the relevant experience and knowledge to enable them to grant authorisations, where an Authorising Officer is newly appointed, the Surveillance Monitoring Officer should be consulted and should approve the authorisation prior to the surveillance commencing.

d. Every application must be properly scrutinised by the Authorising Officer and any applications they consider must be refused must be notified to the Surveillance Monitoring Officer in the way prescribed.

e. Since 1 November 2012, all officer proposals have to be endorsed by the authorising officer and then approved by the Magistrates sitting in the Magistrates' Court. Applications for approval should be made through the legal department.

f. To obtain this approval, the officer requesting the authority must apply to the Magistrates' Court in person for such approval, taking to Court four copies of the officer approved authority for endorsement by the Magistrates Court and which authority should be duly certified as approved on each of the four copies.

g. No action may be taken in reliance upon the authorisation unless and until the Court has approved the authority and it has been so endorsed.

h. Any application for an extension of the authority must be approved by the authorising officer and the Court in the same way. No action should be carried out outside of the approved authority.

i. The authorisation process involves the following steps:

5. **Officers Roles and Procedures.**

Investigation Officer

- A risk assessment will be conducted by the Investigation Officer before an application is drafted and prior to staff being deployed. Lone workers will not undertake surveillance, unless this has been carefully considered and is appropriate to the investigation. This assessment will include the number of officers required for the operation; whether the area involved is suitable for directed surveillance; what equipment might be necessary, health and safety concerns of all those involved and affected by the operation and insurance issues.

- Care must be taken when considering surveillance activity close to schools or in other sensitive areas. If it is necessary to conduct surveillance around school premises, the applicant should inform the head teacher of the nature and duration of the proposed activity, in advance. A Police National Crime database check on those targets should be conducted as part of this assessment. The risk assessment and any notification to a head teacher will be recorded on the case file.

- The Investigation Officer prepares an application. When completing the forms, Investigation Officers must fully set out details of the covert activity for which authorisation is sought to enable the Authorising Officer to make an informed judgment. Consideration should be given to consultation with Legal Services concerning the activity to be undertaken.

- The Investigation Officer will obtain a unique reference number (URN) from the central register, maintained by the RIPA Co-ordinating Officer (RCO) before submitting an application.

- The Investigation Officer will submit the application form to an Authorising officer for approval.

- All applications to conduct directed surveillance (other than under urgency provisions – see below) must be made in writing in the approved format.

Authorising Officer (AO)

- The AO considers the application and if it is considered complete, the application is signed off.

- If there are any deficiencies in the application, further information may be sought from the Investigation Officer, prior to sign off.

- Once final approval has been received, the AO and the Investigation Officer will retain copies and will create an appropriate diary method to ensure that any additional documents are submitted in good time.

- The application form will form the basis of the application to the Magistrates court.

6. Urgent RIPA Applications

- The law has been changed so that urgent cases can no longer be authorised orally. Approval for directed surveillance in an emergency must now be obtained in written form. Oral approvals are no longer permitted. In cases where emergency approval is required an AO must be visited by the applicant with two completed RIPA application forms. The AO will then assess the proportionality, necessity and legality of the application. If the application is approved, then the applicant must then contact the out-of-hours HMCTS representative to seek approval from a Magistrate. The applicant must then take two signed RIPA application forms and the judicial approval form to the Magistrate for the hearing to take place.

- As with a standard application, the test of necessity, proportionality and the crime threshold must be satisfied. A case is not normally to be regarded as urgent unless the delay would, in the judgment of the person giving the authorisation, be likely to endanger life or jeopardise the investigation or operation.

- Examples of situations where emergency authorisation may be sought would be where there is intelligence to suggest that there is a substantial risk that evidence may be lost, a person suspected of a crime is likely to abscond, further offences are likely to take place and/or assets are being dissipated in a criminal investigation and money laundering offences may be occurring. An authorisation is not considered urgent if the need for authorisation has been neglected or the urgency is due to the authorising officer or applicant's own doing.

Authorised activity

- Authorisation takes effect from the date and time of the approval from the Magistrates court.

- Where possible, private vehicles used for directed surveillance purposes should have keeper details blocked.

- Notification of the operation will be made to the relevant police force intelligence units where the target of the operation is in their force area. Contact details for each force intelligence unit should be obtained in advance.

- Before directed surveillance, activity commences, the Investigation Officer will brief all those taking part in the operation. The briefing will include details of the roles to be played by each officer, a summary of the alleged offence(s), the name and/or description of the subject of the directed surveillance (if known), a communications check, a plan for discontinuing the operation and an emergency rendezvous point.

- Where 3 or more officers are involved in an operation, officers conducting directed surveillance will complete a daily log of activity. Evidential notes will also be made in the pocket notebook of all officers engaged in the operation regardless of the number of officers on an operation. These documents will be kept in accordance with the appropriate retention guidelines and Criminal Procedure Investigation Act.

- Where a contractor or external agency is employed to undertake any investigation on behalf of the Council, the Investigation Officer will ensure that any third party is adequately informed of the extent of the authorisation and how they should exercise their duties under that authorisation.

7. Information to be Included in the Application

The written authorisation should specify

(1) identities of the subjects eg names (where known) or descriptions of the subjects and any known history and character thereof (including in cases where investigating officers have reason to believe additional subjects are probable but their identities are unknown they must say so but state their identities are as yet unknown.)

(2) the nature of the surveillance including location of the subject and/or surveillance and (if relevant) the place where CHIS is to be located;

(3) the type of surveillance device or vehicles/equipment to be used;

(4) the type of activities, numbers and names of officers who will be the CHISs (if relevant);

(5) that it is being undertaken for the purpose of preventing or detecting crime or of preventing disorder

(6) that it is proportionate (see definition No.10 in the Definition Section above) i.e. specifying:

(a) the objectives of the surveillance, or the use of a CHIS;

(b) the crime or disorder being investigated (indicate the type of breach);

(c) the likelihood of obtaining private information about a subject or another person(collateral intrusion) and if the likelihood is high/medium /low, how that can be balance against the seriousness of the crime, so if the crime is not serious and there is a high likelihood of personal information being obtained it may not be proportionate to use this method of detection.

(d) the reliability of the intelligence which makes the covert surveillance/CHIS necessary.

(7) The objectives of the activities;

(8) The name and nature of the investigation or operation and what makes the Authorising Officer believe surveillance or the use of a CHIS will achieve the objectives referred to;

(9) The risk of information relating to third parties' private and family life being obtained. This is known as 'collateral intrusion'.

(10) The likelihood of acquiring any confidential/religious material.

8. Obtaining Judicial Authorisation

(a) following approval by the Authorising Officer the Council's Legal Services will contact the Magistrates Court to arrange a hearing. At the same time a copy of the RIPA authorisation and supporting documents setting out the case will be supplied to the Court.

(b) In addition the Authorising Officer should complete a judicial application/order form. The order section of the form will be completed by the JP and will be the official record of the JPs decision.

(c) The Council will need to keep a copy of the judicial application/order form after it has been signed by the JP. The Court will also keep a copy.

(d) Renewals also require JP approval. Cancellations do not require JP approval.

(e) The hearing is a 'legal proceeding' therefore officers must be sworn in and present evidence as required by the JP. The hearing will be in private.

(f) The form for application/order for judicial approval will be kept by the Council's Legal Services.

9. Additional Subjects/Targets

In cases where additional subject/targets may need to be observed the Authorising Officer should state why based on the intelligence relied upon, such additional subjects/targets are considered likely to appear (ie the intelligence behind it) and state that there are further subjects of the investigation whose identities are not yet known e.g. There may be intelligence that a number of youths whose identities are unknown are regularly appearing near a shop or other premises and smashing windows etc. If you state this in the RI Authorisation you are covered for a number of subjects. Then at Renewal stage any such additional targets can be added as and when their identities become known, should it be necessary to do so.

This would not apply where on any one occasion one subject is joined by a further person unexpectedly and it is apparent that he too should be observed but for whom authorisation has not been obtained. Oral authorisation must in this case be obtained as soon as reasonably practicable and the new name (or description) added by means of a further application if a longer period is required.

10. Covert Human Intelligence Sources (CHISs)

Although it is to be hoped that such methods will be rarely used, in addition to the above it is necessary under S29(5) RIPA that there are in force such arrangements as are necessary for ensuring:

(a) that there will at all times be a person holding an office, rank or position with the relevant investigatory authority who will have day to day responsibility for dealing with the CHIS on behalf of that authority and for the CHISs' security and welfare;

(b) that there will at all times be another person holding an office, rank or position with the relevant investigating authority who will have general oversight of the use made of the CHIS;

(c) that there will at all times be a person holding an office, rank or position with the relevant investigating authority who will have responsibility for maintaining a record of the use made of the CHIS;

(d) that the records relating to the CHIS that are maintained by the relevant investigating authority will always contain particulars of all such matters (if any) as may be specified for the purposes of this paragraph in regulations made by the Secretary of State; and

(e) that the records maintained by the relevant investigating authority that disclose the identity of the CHIS will not be available to persons except to the extent that there is a need for access to them to be made available to those persons.

In other words, there must be an officer given direct day to day management of the CHIS to look after his/her needs and another officer in overall control of the use of the CHIS. A record must be made by a specified person of the use of the CHIS. Regulations have been made giving details of the type of particulars needed to be recorded. (See 12 below for details). The identity of CHISs is not to be disclosed unless there is a need to do so. NB - There is no need for 3 different officers. The person responsible for maintaining a record could be the same person with day-to-day responsibility. All relevant Officers involved in the use of CHIS and their management must have the appropriate level of experience and training as may be necessary to undertake the task.

11. Covert Human Intelligence Sources: Criminal Conduct Authorisation Process

First, or at the same time, a use and conduct authorisation under Section 29 of the Regulation of Investigatory Powers Act 2000 (RIPA) (with its necessity and proportionality judgements, must be granted. On top of this, a Criminal Conduct Authorisation (CCA) (must describe why the criminal conduct is necessary for a statutory purpose. The Authorising Officer must consider whether the outcome could be achieved by non-criminal means. The conduct must relate to a specific CHIS, for a specific operation or investigation, and it must be proportionate to what it seeks to achieve.

Taking into account the conditions for granting a CCA, the existing duties to safeguard the CHIS, to make full records, and ensure the CHIS's informed consent, **this means that the authorisation must be clear, specific, time-bound, understood by the CHIS, and the authority must assess that the CHIS is capable of carrying out the activity safely.** Effectively there is a double assessment of aspects of necessity and proportionality, because the CCA must relate to activity which has been authorized under Section 29.

Assessing Proportionality

The draft CHIS Code of Practice mandates proportionality tests including : whether there are reasonable alternatives, and the activity intends to prevent more serious criminality; whether the potential harm to the public interest from the proposed criminal conduct is outweighed by the potential benefit to the public interest; and how the activity will cause the least possible intrusion.

A CCA must comply with the European Convention of Human Rights (ECHR). In addition to the unqualified rights in the ECHR (for instance the right to life and the prohibition on torture and inhuman and degrading treatment and punishment), there are protective obligations on the state. Where the State knows of the existence of a real and immediate threat to a person, the state must take reasonable measures to avoid that risk. No CCA could be granted which did not comply with both the ECHR prohibitions, and its protective duties.

Special safeguards apply to the authorisation of juvenile or vulnerable individuals, and where confidential information (such as legally privileged, or journalistic source information) is likely to be acquired, including a requirement for a higher level of authorisation. These safeguards are sent out in the CHIS Code of Practice.

An enhanced authorisation regime also applies to the use of undercover officers as Relevant Sources as detailed in the Regulation of Investigatory Powers (Relevant Sources) Order 2013. The regime implements the recommendations of HM Inspectorate of Constabulary following the examination of the deployment of a former undercover police officer, but whose findings are applicable to any law enforcement organisation who use undercover officers.

Additional Safeguards

All authorities have **internal disciplinary** procedures. An officer found to be operating in breach of legal or guidance obligations is liable to disciplinary procedure and investigation. This can include criminal investigation. There is an offence of 'Misconduct in a Public Office', which may be relevant to a criminal investigation into such activity, but each investigation will be fact-specific.

There is a duty on all officers involved in exercising the powers in RIPA to inform the Investigatory Powers Commissioner of any **relevant error** in the application of those powers.

12. Records Relating to the CHIS

Records must be kept containing the following by reason of the Regulation of Investigatory Powers (Source Records) Regulations 2000:

(a) the identity of the CHIS;

(b) the identity, where known, used by the CHIS (i.e. his or her 'alias');

(c) any relevant investigating authority other than the authority maintaining the records;

(d) the means by which the CHIS is referred to within each relevant investigating authority (i.e. his or her 'code name');

(e) any other significant information connected with the security and welfare of the CHIS;

(f) any confirmation made by a person granting or renewing an authorisation for the conduct or use of a CHIS that the information in paragraph (d) has been considered and that any identified risks to the security and welfare of the CHIS(s) have where appropriate been properly explained to and understood by the CHIS(s);

(g) the date when, and the circumstances in which, the CHIS was recruited; (or if already employed by the Council and allocated this task);

(i) the identities of the authorising officer and the applicant; the periods during which those persons have discharged those responsibilities;

(j) the tasks given to the CHIS and the demands made of him or her in relation to their activities as a CHIS;

(k) all contacts or communications between the CHIS and a person acting on behalf of any relevant investigating authority;

(l) the information obtained by each relevant investigating authority by the conduct and use of the CHIS;

(m) any dissemination by that authority of information obtained in that way; and

(n) in the case of a CHIS who is not an under-cover operative, every payment, benefit or reward and every offer of a payment, benefit or reward that is made or provided by or on behalf of any relevant investigating authority in respect of the CHIS activities for the benefit of that or any other investigating authority.

Therefore, the officer in charge of maintaining a record of the use of each CHIS should record all these details. The way these records are kept is designed to try to keep the CHIS safe from discovery by the subjects and safe from any harm which could result from their disclosure and also to keep in the open any money or other benefits paid to a CHIS who is not an employee officer of an authorising body.

13. Reviews

Reviews of the authorisation shall be carried out within a period of one month from the date of the authorisation or last review. The Authorising Officer shall carry out the reviews and these reviews must not be confused with authorisations for renewal. The purpose of a review is simply to decide whether or not the activity authorised should continue.

14. Renewals

An Authorising Officer can renew an existing authorisation using Form R3 at any time up to the expiry date of the original authorisation. On or after the expiry date, the authorisation ceases to exist and a new R1 will have to be completed and a new authorisation given.

It is to be noted that renewal is not just a 'rubber stamping' of what has gone before – the requirements of form R3 ensure that the situation is adequately reviewed prior to renewal. An Authorising Officer must not renew an authorisation for the use of a CHIS unless the Authorising Officer is satisfied that a review of certain matters has been carried out and considered the result of that review.

The matters to be reviewed are –

- ***the use made of the source, tasks given to the source and information obtained.***

One useful way of viewing an Authorisation is to regard it as an **insurance policy** – in force only during the times authorised and once expired, it cannot be renewed – it has to be a new application and new policy.

15. Cancellation

The Authorising Officer must cancel an authorisation as soon as if he or she believes that the activity is no longer necessary or proportionate. A cancellation should describe the activity undertaken, explain what was achieved by that activity and give details of the evidence actually obtained. The Authorising Officer should also give instructions regarding the retention, or destruction of the evidence obtained (e. g. video recordings and the like).

An error must be reported as soon as possible and no later than 10 working days after it has been established to the Investigatory Powers Commissioner thatit is a "relevant error". Examples include: Surveillance, property interference or CHIS activity has taken place without lawful authorization or there has been a failure to adhere to the safeguards relating to private information obtained.

16. Errors

Relevant Errors committed by public authorities, in the exercise of their powers and responsibilities under the Investigatory Powers Act 2016, the Regulation of Investigatory Powers Act 2000 and the Police Act 1997, will now need to be reported using the following revised process:

Public authorities must report any Relevant Error to the Investigatory Powers Commissioner (IPC) in accordance with the relevant Code of Practice. All reports should be submitted to Errors@ipco.org.uk.

• Upon receipt of a Relevant Error, an automated acknowledgement will be provided.
• Where any further information or action is required as a result of a Relevant Error report, an IPCO Inspector will make contact with the Council.

• The Relevant Error will then be assessed to determine whether the circumstances could have a) resulted in serious harm or b) call for any urgent changes to national policy or procedures. If this is the case, an investigation will take place.

• If it is not deemed serious, the Relevant Error will be addressed at the Council's next inspection.

Relevant Errors will routinely be examined at each of our inspections.

Public authorities will be required to provide records and confirmation that any material obtained in consequence of the error, that has no connection or relevance to any investigation or operation undertaken by your public au-thority, has been destroyed.

The Senior Responsible Officer for each public authority is responsible for oversight of reporting errors to the IPC, and the identification of both the cause(s) of errors and implementation of processes to minimise repetition.

D. RECORDS

1. Copies of all written authorities, reviews and cancellations should be kept for a period of 5 years after the conclusion of any Court proceedings arising for which the surveillance or use of the CHIS was relevant or until the next visit by the Assistant Surveillance Commissioner whichever is the later.

2. Oral authorisations should be recorded as soon as reasonably practicable after being granted and kept in as D1 above.

3. The Council's Surveillance Monitoring Officer (SMO) is the Executive Director Governance and Resources and Monitoring Officer, whose duty is to retain all original application forms and any other RIPA forms securely. The SMO shall keep a central record of the forms and keep all the forms in a central place. The SMO shall keep the procedure of each covert activity being authorised under review to ensure they comply with the legislation and Codes of Practice and shall meet the Assistant Surveillance Commissioner when he visits the Council to inspect. Also this officer shall be prepared to advise train and assist the Council's officers to enable them to comply with RIPA 2000.

The records shall only be kept for 5 years after the date of expiry and cancellation of the activity, save those cases where legal proceedings have commenced.

4. All information obtained during surveillance should be recorded in writing, in a criminal investigation by means of a surveillance log. This is a form which can be filled in which gives an account of the events observed and conversations heard at particular times which are recorded on the form or log. These should be kept for as long as may be necessary to comply with the Criminal Procedure and Investigations Act 1996 (ie the rules of disclosure in criminal proceedings).

5. All reviews of authorisations must be done in writing and kept as in D1 above as must grounds for withdrawal of authorisation or refusal to renew.

6. At no time must any of the recorded information be disclosed or used except for the purposes for which it was gathered at the time and for use in any future civil or criminal proceedings brought by or against the Council, unless required to do so by the Freedom of Information Act 2000.

7. All information obtained by the CHIS and by the officer responsible for recording the use of the CHIS should be recorded by means of a daily log similar to the surveillance log referred to in 4 above.

8. Such records referred to in 7 above which also reveal the name(s) of the CHIS should only be disclosed if legally necessary or if desired by any Court.

9. Authorising Officers must ensure compliance with the appropriate data protection requirements and the relevant codes of practice and security procedures in the handling and storage of material. Such procedures are essential when preserving continuity of evidence and ensuring admissibility of evidence in Court.

10. Regular reviews of all authorisations should be undertaken during their lifetime to assess the necessity and proportionality of the conduct.

11. Particular consideration should be given in cases where the subject of the investigation or operation might reasonably assume a high degree of confidentiality (legally privileged, confidential journalistic material, constituency business of an MP)

12. Where material has been obtained by surveillance or the use of a source, which is wholly unrelated to a criminal or other investigation or to any person who is the subject of the investigation, and there is no reason to believe it will be relevant to future civil or criminal proceedings, it should be destroyed immediately. Please remember though it is a legal requirement to keep the RIPA forms for 5 years and they must all be given to the Surveillance Monitoring Officer.

13. The mental health and wellbeing of CHIS is a top priority for CHIS units; IPCO continues to engage with those within law enforcement charged with the management of this. IPCO is supporting new processes that are currently on trial and, when on inspection, Inspectors will continue to ensure that issues, risks and needs are identified and addressed appropriately.

SAFEGUARDING AND THE USE OF SURVEILLANCE MATERIAL

14. This section provides guidance on the procedures and safeguards to be applied in relation to the handling of any material obtained through directed surveillance or CHIS activity. This material may include private, confidential or legal privilege information.

15. Dissemination, copying and retention of material must be limited to the minimum necessary for authorised purposes. For the purposes of this code, something is necessary for the authorised purposes if the material:

- Is, or is likely to become, necessary for any of the statutory purposes set out in RIPA in relation to covert surveillance or CHIS activity;
- Is necessary for facilitating the carrying out of the functions of public authorities under RIPA;
- Is necessary for facilitating the carrying out of any functions of the Commissioner or the Investigatory Powers Tribunals necessary for the purposes of legal proceedings; or Is necessary for the performance of the functions of any person by or under any enactment.

16. Material obtained through Directed Surveillance, may be used as evidence in criminal proceedings. The admissibility of evidence is governed primarily by the common law, the Criminal Procedure and Investigations Act 1996 (CPIA), the Civil Procedure Rules, section 78 of the Police and Criminal Evidence Act 1984 and the Human Rights Act 1998.

17. Ensuring the continuity and integrity of evidence is critical to every prosecution Accordingly, considerations as to evidential integrity are an important part of the disclosure regime under the CPIA and these considerations will apply to any material acquired through covert surveillance that is used in evidence. When information obtained under a covert surveillance authorisation is used evidentially, the council will be able to demonstrate how the evidence has been obtained, to the extent required by the relevant rules of evidence and disclosure.

18. Where the product of surveillance could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with established disclosure requirements. In a criminal case the codes issued under CPIA will apply. They require that the investigator record and retain all relevant material obtained in an investigation and later disclose relevant material to the Prosecuting Solicitor. They in turn will decide what is disclosed to the Defence Solicitors.

19. There is nothing in RIPA which prevents material obtained under directed or intrusive surveillance authorisations from being used to further other investigations.All material associated and obtained with an application will be subject to the provisions of the Data Protection Act (DPA) 2018 and CPIA Codes of Practice. All officers involved within this process should make themselves aware of the provisions within this legislation and how it impacts on the whole RIPA process. Material obtained together with relevant associated paperwork should be held securely. Extra care needs to be taken if the application and material relates to a CHIS.

20. Material required to be retained under CPIA should be retained until a decision is taken whether to institute proceedings against a person for an offence or if proceedings have been instituted, at least until the accused is acquitted or convicted or the prosecutor decides not to proceed with the case.

21. Where the accused is convicted, all material which may be relevant must be retained at least until the convicted person is released from custody, or six months from the date of conviction, in all other cases.

22. If the court imposes a custodial sentence and the convicted person is released from custody earlier than six months from the date of conviction, all material which may be relevant must be retained at least until six months from the date of conviction.

23. If an appeal against conviction is in progress when the release, or at the end of the period of six months, all material which may be relevant must be retained until the appeal is determined.

24. If retention is beyond these periods it must be justified under DPA. Each relevant service within the council may have its own provisions which will also need to be considered to ensure that the data is retained lawfully and for as long as is necessary.

25. The Council's Surveillance Monitoring Officer (SMO) is the Executive Director Governance and Resources must ensure compliance with the appropriate data protection requirements under DPA 2018 and any relevant internal arrangements produced by the council relating to the handling and storage of material.

26. It may be necessary to disseminate material acquired through the RIPA covert activity within Tameside Metropolitan Borough Council or shared outside with other councils or agencies,including the Police. The number of persons to whom any of the information is disclosed, and the extent of disclosure, should be limited to the minimum necessary.It must also be in connection with an authorised purpose as set out above. It will be necessary to consider exactly what and how much information should be disclosed. Only so much of the material may be disclosed as the recipient needs; for example, if a summary of the material will suffice, no more than that should be disclosed.

27. The obligations apply not just to Tameside Metropolitan Borough Council as the original authority acquiring the information, but also to anyone to whom the material is subsequently disclosed. In some cases, this will be achieved by requiring the latter to obtain permission from Tameside Metropolitan Borough Council before disclosing the material further. It is important that the Officer In Charge (OIC) of the enquiry considers these implications at the point of dissemination to ensure that safeguards are applied to the data.

28. A record will be maintained justifying any dissemination of material. If in doubt, seek advice from Legal Services.

29. Material obtained through covert surveillance, and all copies, extracts and summaries of it, must be handled and stored securely, to minimise the risk of loss. It must be held to be inaccessible to persons who are not required to see the material (where applicable). This requirement to store such material securely applies to all those who are responsible for the handling of the material. It will be necessary to ensure that both physical and IT security and an appropriate security clearance regime is in place to safeguard the material.

30. Material obtained through covert surveillance may only be copied to the extent necessary for the authorised purposes set out above. 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, and any record which refers to the covert surveillance and the identities of the persons to whom the material relates.

31. In the course of an investigation, Tameside Metropolitan Borough Council must not act on or further disseminate legally privileged items unless it has first informed the Investigatory Powers Commissioner that the items have been obtained.

32. Information obtained through covert surveillance, 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) set out above. 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.

33. Telecommunications data -NAFN

The RIPA (Communications Data) Order 2003 came into law in January 2004. The Investigatory Powers Act 2016 (IPA) came into force for local authorities on Tuesday 11 June 2019. It allows Local Authorities to acquire limited information in respect of subscriber details and service data. It does NOT allow Local Authorities to intercept, record or otherwise monitor communications data.

Applications to use this legislation must be submitted to a Home Office accredited Single Point of Contact (SPOC). The Council uses the services of NAFN (the National Anti-fraud Network) for this purpose.

[1] Consideration of whether or not unrelated material should be destroyed is the responsibility of the Authorising Officer. Only those Officers involved in the investigation are entitled to see the material. In cases where collateral intrusion has taken place, those third parties involved shall not have an automatic right to see the material. (Please note that if they choose to exercise their rights under the Data Protection Act 1998 s7 such request would normally be refused by virtue of s29(3) of the Data Protection Act 1998 if compliance with such a request is likely to prejudice the investigation of a crime.

E. EQUIPMENT

All cctv equipment must be kept securely and a Policy should be adopted by all users of this procedure to ensure the equipment is not used for unauthorised purposes. An example of the type of policy required is on the Council's RIPA intranet site under the heading "POLICY FOR THE RETENTION AND STORAGE OF SURVEILLANCE EQUIPMENT"

F. CIVIL LIABILITY

According to s27(2) of RIPA a person shall not be subject to any civil liability in respect of any conduct of his which is incidental to any conduct which is properly authorised provided it is not of itself conduct for which an authorisation or warrant might reasonably be expected to have been obtained under another enactment. An example is where a RIPA authorisation is granted to put a tracking device on a private vehicle. This could give rise to civil liability because a 'property interference authorisation" under the Police Act 1997 is necessary.

Of course if not properly authorised a person could incur personal liability and face disciplinary action.

G. COMPLAINTS

Any complaints about any powers covered by this Procedural Guide can either be made under the Council's existing corporatel complaints system or to the Investigatory Powers Tribunal set up under S65 RIPA 2000.

H. 1 FORMS FOR DIRECTED SURVEILLANCE

NB. All forms are on the Council's intranet site – do not save them as they may be updated and you need to ensure it is the most up-to-date copy. **Users must access the forms from the intranet site every time without fail.**

R1/DS Application for authorisation, authorisation form and record of grant of oral authorisation

R2/DS Review form

R3/DS Application for renewal of authorisation and renewed authorisation

R4/DS Cancellation form

H 2 FORMS FOR COVERT HUMAN INTELLIGENCE SOURCES

R1/CHIS Application for authorisation, authorisation form and record of grant of oral authorisation

R2/CHIS Review form

R3/CHIS Application for renewal of authorisation and renewed authorisation

R4/DS Cancellation form

H.3 FORMS FOR DIRECTED SURVEILLANCE AND CHIS

R5/DS/CHIS Authorisation control sheet for both directed surveillance and CHIS's

For ease of reference these are named forms R1-5. If it is for directed surveillance it has the initials DS after the letter R; if for a CHIS, it has CHIS.

I. THE APPLICATION AND AUTHORISATION FORMS

1. **The application**

1. R1, the **main application form**, should be completed by the Investigating Officer who wants to apply to the Authorising Officer for authorisation in every case and should also be completed in retrospect as soon as reasonably practicable after an oral authorisation is granted as a record of the grant of oral authorisation.

2. R1 must also be read and signed by the Authorising Officer and completed by him and signed when urgent Oral Authorisation has been granted. If he wishes to refuse the application he can do so by striking it through twice in black, notifying the Investigating Officer and sending it to the SMO with a note of reasons.

3. The application for **renewal** of authorisation R3 should be completed by the Officer in cases where written authorisation is about to end should it be necessary and proportionate to carry on the surveillance or use of CHIS beyond the time when it is due to end. R3 should then be completed by the Authorising Officer.

4. The review form R2 should be completed by the Authorising Officer at regular intervals of his own choosing or whenever the surveillance which has been authorised continues longer than one month. This is where the authorisation control sheet R5 is useful as evidence that reviews have been carried out.

5. A cancellation form R4 should be completed in full in all cases where the Authorising Officer considers that the directed surveillance or use of CHIS is no longer necessary or proportionate.

6. The authorisation control sheet R5 is essential as a monitoring tool for the authorising officer.

7. The Surveillance Monitoring Officer (SMO) has to maintain a central record sheet of all authorisations which needs to be kept up to date. Authorising Officers need to forward all completed forms to the SMO immediately so that they can be recorded immediately or at least no later than 48 hours after the date of the authorisation.

8. Any applications for authorisation that are refused by the Authorising Officer should be struck out with two black lines through and stamped "REFUSED". All such refusals should be forwarded to the Surveillance Monitoring Officer to be recorded accordingly, with an accompanying note stating reasons for the refusal.

NB Such applications for authorisation are important and must not be taken lightly. Time needs to be set aside for proper consideration of the matter by both Investigating and Authorising Officers and, if in doubt about any of the legal aspects and the applicability of RIPA to a given situation, advice should be sought from the Surveillance Monitoring Officer.

RESOURCES

Full Codes of Practice can be found on the Home Office website:

http://www.homeoffice.gov.uk/

- **Covert Surveillance & Property Interference:**

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742041/201800802_CSPI_code.pdf

- **CHIS:**

https://www.gov.uk/government/consultations/revised-covert-human-intelligence-source-chis-code-of-practice

Acquisition and Disclosure of Communications Data:

https://www.gov.uk/government/publications/code-of-practice-for-the-acquisition-and-disclosureofcommunications-data

- Further information can also be found on The IPCO website:

https://www.ipco.org.uk/

J. PRACTICAL EXAMPLES, GUIDANCE AND ADVICE IN SPECIFIED CIRCUMSTANCES

A. GENERAL

Detailed guidance is set out in the Home Office Guidance and Office of Surveillance Commissioners (OSC) Procedures and Guidance to which all officers have access, and if unable to locate should contact Legal Services for assistance.

Below are some examples taken from the OSC Procedures and Guidance. Officers should familiarise themselves with the contents of this guidance, and its applicability to their activities.

To recap, surveillance, for the purpose of the 2000 Act, includes monitoring, observing or listening to persons, their movements, conversations or other activities and communications. It may be conducted with or without the assistance of a surveillance device and includes the recording of any information obtained.

Surveillance is covert if, and only if, it is carried out in a manner calculated to ensure that any persons who are subject to the surveillance are unaware that it is or may be taking place.

Specifically, covert surveillance may be authorised under the 2000 Act if it is either directed or intrusive:

Directed surveillance is covert surveillance that is not intrusive and is carried out in relation to a specific investigation or operation in such a manner as is likely to result in the obtaining of private information about any person (other than by way of an immediate response to events or circumstances such that it is not reasonably practicable to seek authorisation under the 2000 Act);

Intrusive surveillance is covert surveillance that is carried out in relation to anything taking place on residential premises or in any private vehicle (and that involves the presence of an individual on the premises or in the vehicle or is carried out by a means of a surveillance device)

Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public 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 future consideration or analysis. Surveillance of publicly accessible areas of the internet should be treated in a similar way, recognising that there may be an expectation of privacy over information which is on the internet, particularly where accessing information on social media websites.

Example: *Two people holding a conversation on the street or in a bus may have a reasonable expectation of privacy over the contents of that conversation, even though they are associating in public. The contents of such a conversation should therefore still be considered as private information. A directed surveillance authorisation would therefore be appropriate for a public authority to record or listen to the conversation as part of a specific investigation or operation.*

Example: *Officers of a local authority wish to drive past a café for the purposes of obtaining a photograph of the exterior. Reconnaissance of this nature is not likely to require a directed surveillance authorisation as no private information about any person is likely to be obtained or recorded. However, if the authority wished to conduct a similar exercise, for example to establish a pattern of occupancy of the premises by any person, the accumulation of information is likely to result in the obtaining of private information about that person and a directed surveillance authorisation should be considered.*

The fact that a directed surveillance authorisation is available does not mean it is required. There may be other lawful means of obtaining personal data which do not involve directed surveillance.

Example: A surveillance officer intends to record a specific person providing their name and telephone number to a shop assistant, in order to confirm their identity, as part of a criminal investigation. Although the person has disclosed these details in a public place, there is nevertheless a reasonable expectation that the details are not being recorded separately for another purpose. A directed surveillance authorisation should therefore be sought.

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

As set out in paragraph 3.14 of the August 2018 revised code, depending on the nature of the online platform, there may be a reduced expectation of privacy where information relating to a person or group of people is made openly available within the public domain, however in some circumstances privacy implications still apply. This is because the intention when making such information available was not for it to be used for a covert purpose such as investigative activity. This is regardless of whether a user of a website or social media platform has sought to protect such information by restricting its access by activating privacy settings.

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

Whether a public authority interferes with a person's private life includes a consideration of the nature of the public authority's activity in relation to that information. Simple reconnaissance of such sites (i.e. preliminary examination with a view to establishing whether the site or its contents are of interest) is unlikely to interfere with a person's reasonably held expectation of privacy and therefore is not likely to require a directed surveillance authorisation. But where a public authority is systematically collecting and recording information about a particular person or group, a directed surveillance authorisation should be considered. These considerations apply regardless of when the information was shared online. See also paragraph 3.6 of the August 2018 revised 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* 20 *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.*

- Whether the information obtained will be recorded and retained;
- Whether the information is likely to provide an observer with a pattern of lifestyle;
- Whether the information is being combined with other sources of information or 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.

Example: *An authorisation under the 2000 Act would not be appropriate where police officers conceal themselves to observe suspicious persons that they come across in the course of a routine patrol or monitor social media accounts during a public order incident.*

Example 1: *Plain clothes police officers on patrol to monitor a high street crime hot-spot or prevent and detect shoplifting would not require a directed surveillance authorisation. Their objective is merely to observe a location and, through reactive policing, to identify and arrest offenders committing crime. The activity may be part of a specific investigation but is general observational activity, rather than surveillance of individuals, and the obtaining of private information is unlikely. A directed surveillance authorisation need not be sought.*

Example 2: *Police officers monitoring publicly accessible information on social media websites, using a general search term (such as the name of a particular event they are policing), would not normally require a directed surveillance authorisation. However, if they were seeking information relating to a particular individual or group of individuals, for example, by using the search term "group x" (even where the true identity of those individuals is not known) this may require authorisation. This is because use of such a specific search term indicates that the information is being gathered as part of a specific investigation or operation, particularly in circumstances where information is recorded and stored for future use.*

Example 3: *Local authority officers attend a car boot sale where it is suspected that counterfeit goods are being sold, but they are not carrying out surveillance of particular individuals and their intention is, through reactive policing, to identify and tackle offenders. Again this is part of the general duties of public authorities and the obtaining of private information is unlikely. A directed surveillance authorisation need not be sought.*

Example 4: *Intelligence suggests that a local shopkeeper is openly selling alcohol to underage customers, without any questions being asked. A trained employee or person engaged by a public authority is deployed 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 in regards to the requirements of the Act, that a public authority may conclude that a CHIS authorisation is unnecessary. However, if the test purchaser is wearing recording equipment and is not authorised as a CHIS, or an adult is observing, consideration should be given to granting a directed surveillance authorisation.*

Example 5: *Surveillance officers intend to follow and observe Z covertly as part of a pre-planned operation to determine her suspected involvement in shoplifting.*

It is proposed to conduct covert surveillance of Z and record her activities as part of the investigation. In this case, private life considerations are likely to arise where there is an expectation of privacy and the covert surveillance is pre-planned and not part of general observational duties or reactive policing. A directed surveillance authorisation should therefore be considered.

The 'core functions' referred to by the Investigatory Powers Tribunal are the 'specific public functions', undertaken by a particular public authority, in contrast to the 'ordinary functions' which are those undertaken by all authorities (e.g. employment issues, contractual arrangements etc.). These "ordinary functions" are covered by the Data Protection Act 2018 and the Information Commissioner's Employment Practices Code. A public authority may only seek authorisations under the 2000 Act when in performance of its 'core functions'. For example, the disciplining of an employee is not a 'core function', although related criminal investigations may be. As a result, the protection afforded by an authorisation under the 2000 Act may be available in relation to associated criminal investigations, so long as the activity is deemed to be necessary and proportionate.

Example 1: *A police officer is suspected by his employer of undertaking additional employment in breach of discipline regulations. The police force of which he is a member wishes to conduct covert surveillance of the officer outside the police work environment. Such activity, even if it is likely to result in the obtaining of private information, does not constitute directed surveillance for the purposes of the 2000 Act as it does not relate to the discharge of the police force's core functions. It relates instead to the carrying out of ordinary functions, such as employment, which are common to all public authorities.*

Example 2: *A police officer is suspected to be removing classified information from the work environment and sharing it improperly. The police force wishes to investigate the matter by undertaking covert surveillance of the employee. The misconduct under investigation amounts to the criminal offence of misfeasance in a public office, and therefore the proposed investigation relates to the core functions of the police, and the proposed surveillance is likely to result in the obtaining of private information. Consequently, a directed surveillance authorisation should be considered*

Example 3: *It is alleged that a public official has brought their department into disrepute by making defamatory remarks online, and identifying themselves as a public official. The department wishes to substantiate the allegations separately from any criminal action. Such activity, even if it is likely to result in the obtaining of private information, does not constitute directed surveillance for the purposes of the 2000 Act, as it does not relate to the discharge of the department's core functions.*

Necessity and proportionality

The following elements of proportionality should therefore be considered:

- balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or harm;
- explaining how and why the methods to be adopted 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 information sought;
- evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented, or have been implemented unsuccessfully.

The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012 has the following effects:

- Local authorities in England and Wales can only authorise use of directed surveillance under RIPA to prevent or detect criminal offences that are either punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months' imprisonment **or** are related to the underage sale of alcohol and tobacco or nicotine inhaling products. The offences relating to the latter are in article 7A of the 2010 RIPA Order.

- Local authorities **cannot** authorise directed surveillance for the purpose of preventing disorder unless this involves a criminal offence(s) punishable (whether on summary conviction or indictment) by a maximum term of at least 6 months' imprisonment.

- Local authorities may therefore continue to authorise use of directed surveillance in more serious cases as long as the other tests are met – i.e. that it is necessary and proportionate and where prior approval from a JP has been granted.

B. Specific Examples

1. Use of Social Networking Sites (SNS)

See 3.10 to 3.17 of Covert Surveillance and Property Interference Revised Code of Practice August 2018

The internet may be used for intelligence gathering and/or as a surveillance tool, and it is important that public authorities are able to make full and lawful use of this information for their statutory purposes. Much of it can be accessed without the need for RIPA authorisation.

However, the fact that digital investigation is routine or easy to condone does not reduce the need for authorisation in relevant circumstances.

Care must be taken to understand how the SNS works. Authorising officers must not be tempted to assume that one service provider is the same as another or that the services provided by a single provider are the same.

Whilst it is the responsibility of an individual to set privacy settings to protect unsolicited access to private information, and even though data may be deemed published and no longer under the control of the author, it is unwise to regard it as 'open source' or publicly available; the author has a reasonable expectation of privacy if access controls are applied.

In some cases data may be deemed private communication still in transmission (instant messages for example). Where privacy settings are available but not applied the data may be considered open source and an authorisation is not usually required.

Directed Surveillance: Providing there is no warrant authorising interception in accordance with section 48(4) of the 2000 Act, if it is necessary and proportionate for a public authority to breach covertly access controls, the minimum requirement is an authorisation for directed surveillance.

CHIS: An authorisation for the use and conduct of a CHIS is necessary if a relationship is established or maintained by a member of a public authority or by a person acting on its behalf (ie the activity is more than mere reading of the site's content).

It is not unlawful for a member of a public authority to set up a false identity but it is inadvisable for a member of a public authority to do so for covert purposes without authorisation. Using photographs of other persons without their permission to support the false identity infringes the law.

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 (ie the person from whom consent is sought must agree (preferably in writing) what is and is not to be done)."

2. Updating photographs for intelligence purposes

Covertly taking a photograph for the purpose of updating records is capable of being directed surveillance and should be authorised.

3. Covert surveillance of co-habiting couples

The purpose of surveillance is to investigate a crime and not a criminal. It is usually not possible to be certain of a partner's awareness of a criminal situation and proving awareness of a criminal situation and proving co-habitation is sometimes necessary and proportionate. It is appropriate subject to accurately constructed documents, to authorise surveillance against co-habiting parties. Authorising Officers should confine surveillance of the partner to that which is necessary to prove co-habitation. Surveillance of juveniles or other family members should be avoided.

4. The availability of resources

Whilst there may be a public expectation that public bodies will monitor offenders, an Authorising Officer should not grant an activity when he knows there to be insufficient covert surveillance resource to conduct it.

5. Technical feasibility studies

Feasibility studies should be conducted before the application is submitted to the Authorising Officer. Without it the Authorising Officer is unable to know the objectives can be achieved or to accurately assess proportionality or collateral intrusion. Ii is unacceptable to deny knowledge of technical capability from the Authorising Officer.

6. Private information

An authorisation for directed surveillance is required whenever it is believed that there is a real possibility that the manner in which is is proposed to carry out particular surveillance will result in the obtaining of private information about any person, whether or not that person is or becomes a subject of the operation.

7. Use of noise monitoring equipment

Measuring levels of noise audible in the complainant's premise is not surveillance because the noise has been inflicted by the perpetrator who has probably forfeited any claim to privacy.

Using sensitive equipment to discern speech or other noisy activity not discernible by the unaided ear is covert, likely to obtain private information and may be intrusive surveillance.

The Authorising Officer should consider whether the surveillance equipment is capable of measuring volume only or whether it can identify the perpetrators, mindful that the more sensitive the equipment the greater the potential for intrusive surveillance.

Where possible, the intention to monitor noise should be notified to the owner and occupier of the premises being monitored.

Where notice is not possible or has not been effective, covert monitoring may be considered necessary and proportionate. If monitoring equipment is used as a means also to assess whether a claim is vexatious, any consent provided by the complainant to use monitoring equipment on his premises is vitiated of the capability of the equipment is not explained.

8. CCTV and ANPR systems

It is recommended that a law enforcement agency should obtain a written protocol with a local authority if the latter's CCTV system is to be used for directed surveillance. Any such protocol should be drawn up centrally in order to ensure a unified approach.

The protocol should include a requirement that the local authority should see the authorisation (redacted if necessary to prevent the disclosure of sensitive information) and only allow its equipment to be used in accordance with it.

The use of overt CCTV cameras by public authorities does not normally require an authorisation under the 2000 Act e.g by virtue of visible signage/cameras, information and undertaking consultation.

Guidance on their operation is provided in the Surveillance Camera Code of Practice, overseen by the Surveillance Camera Commissioner. Regard should also be had to the Commissioner's Code, 'in the Picture – A Data Protections Code of Practice for Surveillance Cameras and Personal Information'.

The Surveillance Camera code sets out a framework of good practice that includes existing legal obligations, including the processing of personal data under the Data Protection Act 2018 and a public authority's duty to adhere to the Human Rights Act 1998. Similarly, the overt use of ANPR systems to monitor traffic flows or detect motoring offences does not require an authorisation under the 2000 Act.

Example: *Overt surveillance equipment, such as town centre CCTV systems or ANPR, is used to gather information as part of a reactive operation (e.g. to identify individuals who have committed criminal damage after the event). Such use does not amount to covert surveillance as the equipment was overt and not subject to any covert targeting. Use in these circumstances would not require a directed surveillance authorisation.*

However where overt CCTV, ANPR or other overt surveillance cameras are used in a covert and planned manner as part of a specific investigation or operation, for the surveillance of a specific person or group of people, a directed surveillance authorisation should be considered. Such covert surveillance is likely to result in the obtaining of private information about a person (namely a record of their movements and activities) and therefore falls properly within the definition of directed surveillance . The use of the CCTV, ANPR or other overt surveillance cameras in these circumstances goes beyond their intended use for the general prevention or detection of crime and protection of the public.

Example: *A local police team receive information that an individual suspected of committing thefts from motor vehicles is known to be in a town centre area. A decision is taken to use the town centre CCTV system to conduct surveillance against that individual, such that he remains unaware that there may be any specific interest in him. This targeted, covert use of the overt town centre CCTV system to monitor and/or record that individual's movements should be considered for authorisation as directed surveillance.*

9. Test purchases of sales to juveniles

Guidance is given in respect of undertaking test purchasing operations by the Code of Practice: Age Restricted Products published by BIS/BRDO in 2014.

The BIS/BRDO guidance states that an enforcing authority should consider the statutory requirements for authorization under RIPA when conducting test purchase operations. The application of RIPA to test purchasing has been debated for some time with guidance and clarification being sought from a number of sources:

Test purchase activity does not in general require authorization as a CHIS under RIPA as vendor-purchaser Test purchase activity does not in general require authorisation as a CHIS under RIPA as vendor-purchaser activity does not normally constitute a relationship as the contact is likely to be so limited. However, if a number of visits are undertaken at the same establishment to encourage familiarity, a relationship may be established and authorisation as a CHIS should be considered.

If the test purchaser is wearing recording equipment and is not authorised as a CHIS, or an adult is observing, consideration should be given to granting a directed surveillance authorisation. The Home Office Code of Practice for Covert Surveillance and Property Interference (December 2014)

The ECHR has construed the manner in which a business is run as private information [see also Covert Surveillance and Property Interference Code of Practice paragraphs 2.5 and 2.6] and such authorisation must identify the premises involved.

When conducting covert test purchase operations at more than one establishment, it is not necessary to construct an authorisation for each premise to be visited but the intelligence must be sufficient to prevent “fishing trips”. Premises may be combined within a single authorisation provided that each is identified at the outset. Necessity, proportionality, and collateral intrusion must be carefully addressed in relation to each of the premises. It is unlikely that authorisations will be considered proportionate without demonstration that overt methods have been considered or attempted and failed. (Sec 245 OSC Procedures & Guidance 2016)

In all cases a prior risk assessment is essential in relation to the young person.

10. Risk Assessments

The authorisation request should be accompanied by a risk assessment, giving details of how the CHIS is going to be handled and the arrangements which are in place for ensuring that there is at all times a person with responsibility for maintaining a record of the use made of CHIS. The risk assessment should take into account the safety and welfare of the CHIS in relation to the activity and should consider the likely consequences should the role of the CHIS become known. The ongoing security and welfare of the CHIS after the cancellation of the authorization should also be considered at the outset.

It is unlikely that authorisations will be considered proportionate without demonstration that overt methods have been considered or attempted and failed.

11. Drones

Where surveillance using airborne crafts or devices, for example helicopters or unmanned aircraft (colloquially known as ‘drones’), is planned, the same considerations outlined in chapters 3 and 5 of the August 2018 code should be made to determine whether a surveillance authorisation is appropriate. In considering whether the surveillance should be regarded as covert, account should be taken of the reduced visibility of a craft or device at altitude. (See also 3.36 to 3.39 of this code with regard to overt surveillance cameras.)

Example: *An unmanned aircraft deployed by a police force to monitor a subject of interest at a public demonstration is likely to require an authorisation for directed surveillance, as it is likely that private information will be obtained and those being observed are unaware it is taking place, regardless of whether the drone is marked as belonging to the police force. Unless sufficient steps have been taken to ensure that participants in the demonstration are aware that aerial surveillance will be taking place, such activity should be regarded as covert.*

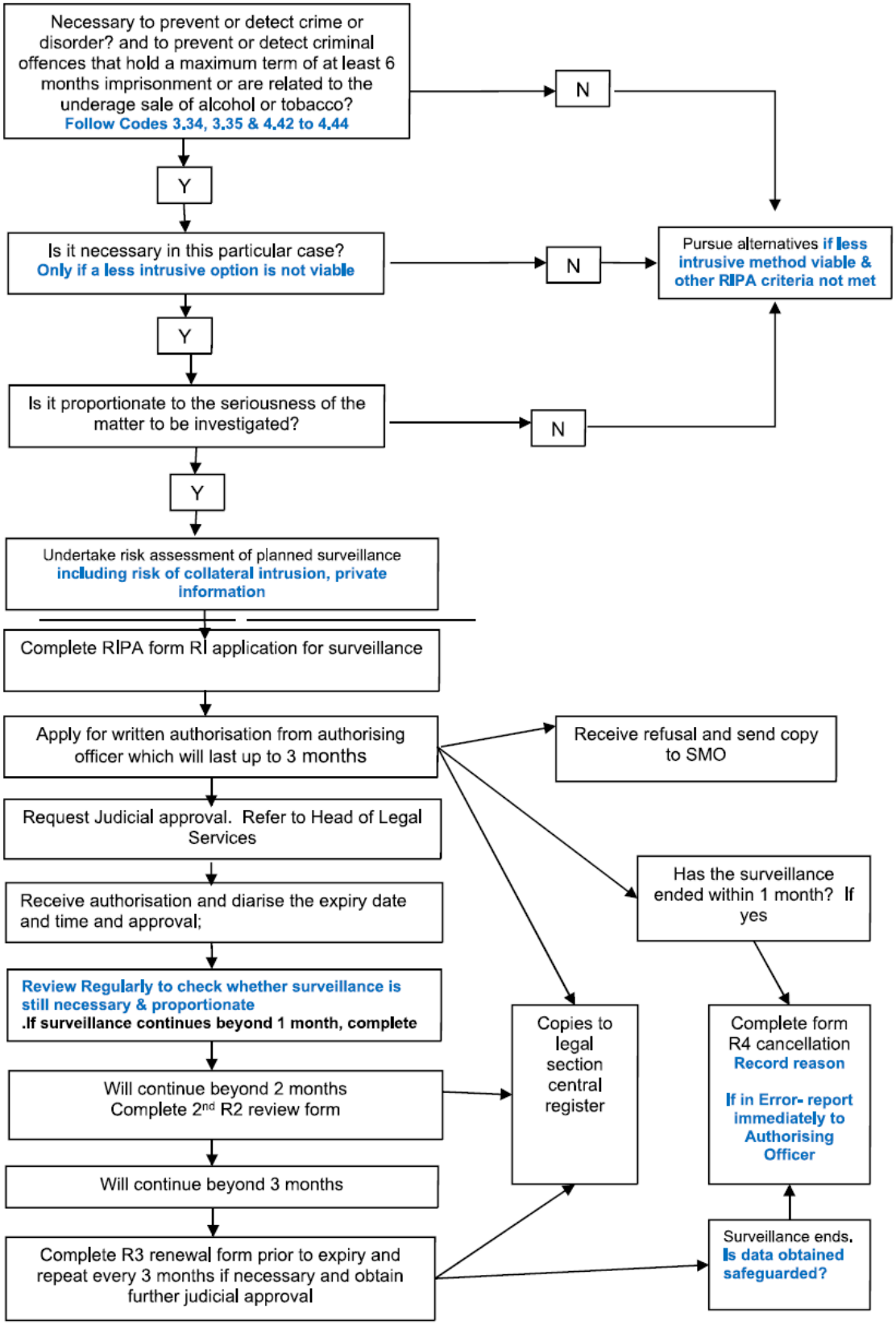
Example: *An observation post outside residential premises which provides a limited view compared to that which would be achievable from within the premises does not constitute intrusive surveillance. However, the use of a zoom lens, for example, which consistently achieves imagery of the same quality as that which would be visible from within the premises, would constitute intrusive surveillance.*

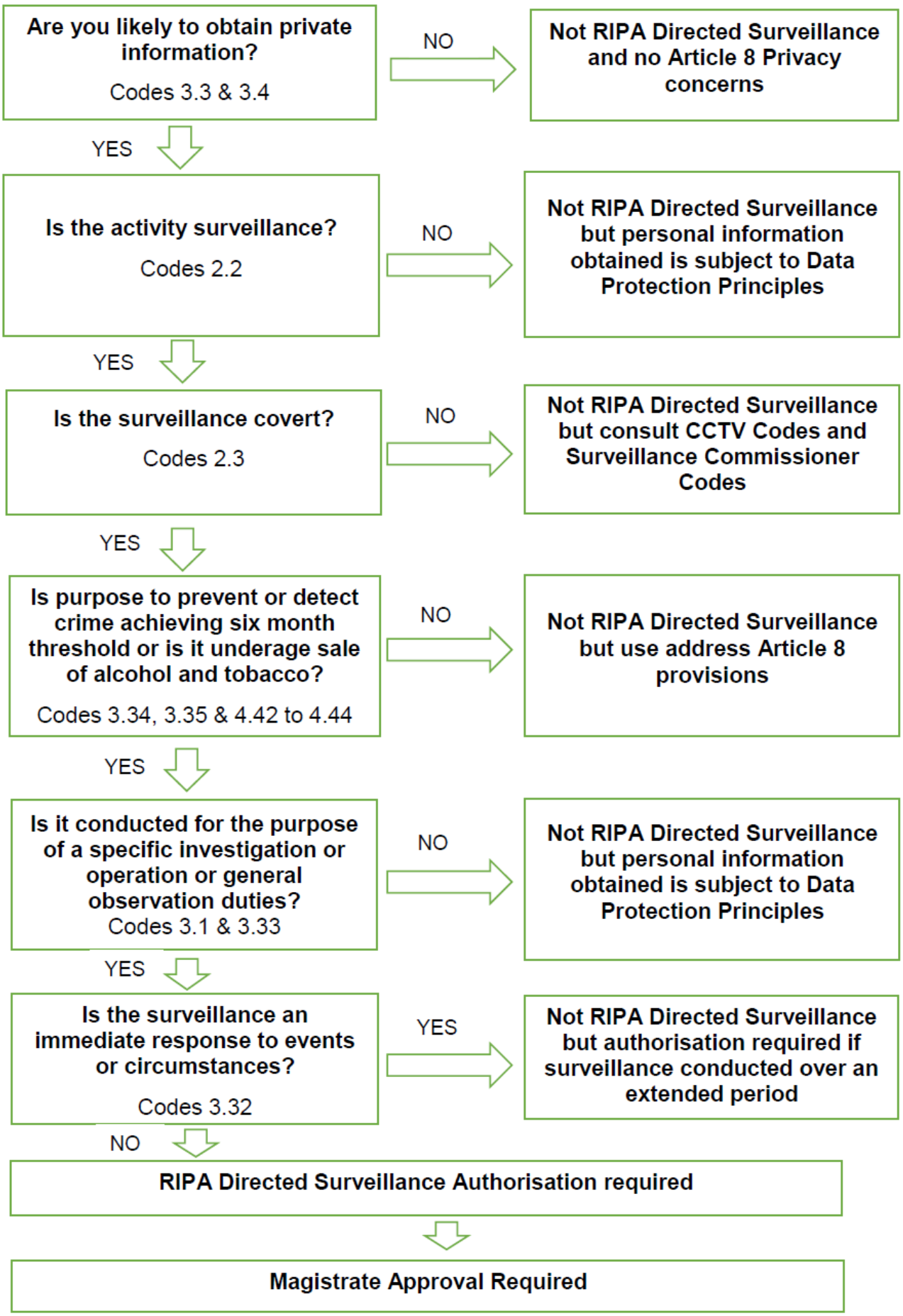
12. Researchers

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.*

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 (see paragraphs 3.6 and 4.32 of the August 2018 revised code). Consideration should be given as to whether it is likely to result in obtaining private information about a person or group.

K. RIPA SURVEILLANCE APPLICATIONS PROCESS MAP – DIRECTED SURVEILLANCE




Are you likely to obtain private information?
Codes 3.3 & 3.4
NO
Not RIPA Directed Surveillance and no Article 8 Privacy concerns
YES
Is the activity surveillance?
Codes 2.2
NO
Not RIPA Directed Surveillance but personal information obtained is subject to Data Protection Principles
YES
Is the surveillance covert?
Codes 2.3
NO
Not RIPA Directed Surveillance but consult CCTV Codes and Surveillance Commissioner Codes
YES
Is purpose to prevent or detect crime achieving six month threshold or is it underage sale of alcohol and tobacco?
Codes 3.34, 3.35 & 4.42 to 4.44
NO
Not RIPA Directed Surveillance but use address Article 8 provisions
YES
Is it conducted for the purpose of a specific investigation or operation or general observation duties?
Codes 3.1 & 3.33
NO
Not RIPA Directed Surveillance but personal information obtained is subject to Data Protection Principles
YES
Is the surveillance an immediate response to events or circumstances?
Codes 3.32
YES
Not RIPA Directed Surveillance but authorisation required if surveillance conducted over an extended period
NO
RIPA Directed Surveillance Authorisation required
Magistrate Approval Required