I am writing to request the following information under the FOI Act.

1) A copy of your corporate policy on the use of social media in investigations. (please state if you do not have one). Please include any additional guidance/code of practice for this activity when it includes the monitoring or accessing of information published on social media that is either publicly available or requires additional access e.g. to be 'friends' with an individual, to have password and login details.	A copy of the Council's Regulation of Investigatory Powers Policy is attached which includes guidance on the use of Social Media
2) Does your Local Authority conduct overt and/or covert social media intelligence and/or monitoring? If the answer is yes, please explain what types– e.g. profiling individuals, conducting investigations, monitoring individuals/groups/ locations – if possible, state the purpose of such activity and how regularly it is used, including any recent relevant figures (for the last five calendar years, if available).	Yes- to investigate complaints of sales of counterfeit goods /illicit tobacco/ unregistered tattooists/ unregistered dog breeders. Records are available from 2019: 82 activities
3) If the Local Authority has conducted covert social media monitoring, please confirm the number of RIPA warrants obtained in the last five calendar years for this purpose. (2017-18, 2018-19, 2019-20, 2020-21, 2021-22).	None
4) Please confirm whether or not your local authority has purchased or uses software and/or hardware to conduct social network / social media monitoring and/or in relation to sentiment analysis.	The Council has not purchased or use such equipment
5) If you answered yes to 4), please state the name of the company or provider.	N/A
6) If you answered no to 4), please, please state whether the local authority has developed internal methods to conduct social media / social network monitoring and be as specific as you can about these methods– when and how they are used and what happens to any data gathered.	The Council is withholding this information under s31 of FOIA. Disclosure under FOIA is considered to be to the public at large. Covert surveillance is used for the detection and prevention of crime. Disclosure will prejudice the prevention and detection of crime ; alert the public / criminals to what methods are used. The Council has considered the public interest test. The council has balanced the public interest in understanding how covert surveillances are undertaken and action the authority takes to prevent crime against the need to ensure that the Council's activities to prevent and detect crime are not undermined . On balance the Council believes that the need to protect the public by engaging in crime detection and prevention is the greater need believing that if its methods of covert surveillance were made known to the public at large, detection and prevention would be adversely affected.

WIGAN BOROUGH COUNCIL

P R O C E D U R A L G U I D E

FOR THE USE OF COVERT SURVEILLANCE AND COVERT HUMAN INTELLIGENCE SOURCES ("CHIS") AND THE ACCESSING OF COMMUNICATIONS DATA INCLUDING NON-RIPA SURVEILLANCE

Revised June 2022

To comply with the Regulation of Investigatory Powers Act 2000 and 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

I N D E X

A. GENERAL INTRODUCTION

1. This Procedural Guide along with the statutory Codes of Practice published by the Secretary of State must be readily available at Wigan Borough Council, Resources Directorate, Legal Division, Town Hall (hereinafter referred to as WBC) for consultation and reference by Investigating Officers, Members of the Council, the public and/or their representatives. These documents can be obtained from the –RIPA Monitoring Officer, Town Hall, Library Street, Wigan WN1 1YN

2. This Procedural Guide applies to any covert surveillance, use of Covert Human Intelligence Sources ('CHISs') or the accessing of communications data by WBC employees whose duties include investigation under properly delegated powers and by private investigators engaged to act as agents by those WBC employees. It should be emphasised that the Regulation of Investigatory Powers Act 2000 (RIPA) will only apply if the surveillance or use of CHIS is "covert". Quite often such activities will be done overtly, and fall outside RIPA, so it is advisable to be familiar with the definition of "covert" under RIPA as a starting point. There will also be certain types of covert surveillance that does not fall within the RIPA regime. In those circumstances officers are advised to follow the procedure outlined within this Guide at Para G that mirrors the scheme as far as possible. This approach will have particular application in connection with covert surveillance that could be interpreted as intruding upon human rights such as employee monitoring or surveillance in connection with civil county court claims.

3. This Procedural Guide has been drafted for Wigan Borough Council and has regard to the provisions of the Codes of Practice and additional Supplemental Guidance issued by the Secretary of State under Section 71 RIPA. It should be noted that Section 72(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. Codes of Practice can be found at www.gov.uk. This Guide has been compiled for Wigan Borough Council only omitting elements which are not applicable to this Council. For example, there is no power of authorisation for 'intrusive surveillance' (see definition B8 in this Guide) so references to such authorisations have been omitted. There is also no power to engage in property interference. This includes the use of tracking or recording devices inserted into vehicles either directly or indirectly.

4. All covert surveillance, use of CHISs or the accessing of communications data should be authorised or conducted in accordance with this Procedural Guide and should be carried out only for the purpose of preventing or detecting crime which the Council is legally required or legally empowered to investigate as part of its functions. In addition, covert surveillance may only be authorised if the criminal offence which is sought to be prevented or detected is punishable on conviction a maximum term of at least six months of imprisonment, or would constitute an offence under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933 (offences involving sale of tobacco and alcohol to underage children). This restriction does not apply to the use of CHISs or the accessing of communications data.

5. Covert surveillance, the use of CHISs and the accessing of communications data should only be used by the Council where it believes it is "necessary" and "proportionate" (see definitions section below).

6. Before authorising covert surveillance Authorising Officers should 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. If there is a risk of obtaining confidential material as defined in section 83 of RIPA it is necessary to obtain authorisation from the Chief Executive or the Deputy Chief Executive.

7. As far as surveillance is concerned this Procedural Guide 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 in accordance with their authorisation procedure. All surveillance operations in which the surveillance is likely to be intrusive need prior authorisation by the Chief Constable of Police and can only be carried out in cases where it is for the prevention and detection of "serious crime" (see B14 in the Definitions section below).

8. For the avoidance of doubt surveillance notified to the subject, in certain circumstances may not be covert such that it would not fall within the provisions of this Procedural Guide. Much will depend on:

   - what surveillance the subject was informed would be undertaken
   - how the notification was delivered;
   - the time lapse between notification and surveillance
   - whether the surveillance undertaken was within what the subject was informed would be undertaken

   Also, 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 are made when overtly looking or asking questions, then such actions are usually already authorised specifically by other legislation in any event.

9. Common-sense dictates that surveillance will not be undertaken from, for instance a property 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. **IPCO** – The IPCO (Investigative Powers Commissioners Office) does not give legal advice and any opinion given should not be cited as definitive advice from the IPCO. In the event that guidance is required it is usual to take advice from the RIPA Monitoring Officer in the first instance. In the event that a further opinion becomes necessary it will be for the Senior Responsible Officer alone to seek further guidance from the IPCO. It is not envisaged that a reference of this nature will be routine and will be reserved for questions of significant importance where there is little or no official guidance or case law.

11. <u>Working with other agencies</u>

    In the event that surveillance takes place in conjunction with other agencies Council officers should normally be authorised in accordance with our own procedures. In the event that the source of the authorisation is the other agency it will be the responsibility of the line manager of the operative to obtain a copy of the authorisation. He will also liaise with his own operatives to ensure compliance with that authorisation and cause a copy of it to be lodged at the central record.

B. DEFINITIONS

1. Authorising Officer

At or higher than "An Assistant Chief Officer, Assistant Head of Service, Service Manager or equivalent" (Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010). Therefore, for the purposes of this Procedural Guide the Authorising Officers shall be the persons appointed by the Council's Senior Responsible Officer (SRO) at any particular time to hold such a position across the Council's departments. If knowledge of confidential information is likely to be acquired, or a person under the age of 18 or a vulnerable individual is to be used as a CHIS, then the authorising officer must be the Council's Chief Executive or (in his/her absence) the Deputy Chief Executive.

All decisions made by an Authorising Officer should be made on facts and evidence. Decisions based mainly on inadmissible hearsay and intelligence are not likely to be satisfactory unless there is reason to believe that the material is reliable. The Authorising Officer should set out the reasons why he is satisfied or why he believes that the authorisation is **both** necessary and proportionate. It should be clear from this narrative that the officer understands the difference between the two concepts and has applied his mind judicially. It is the responsibility of the Authorising Officer to ensure that all operatives are fully aware of the scope and limits of the surveillance authorisation.

The current list of Authorising Officers, maintained by the RIPA Monitoring Offficer, is attached at Appendix A.

2. Communications Data

This includes information relating to the use of a postal service or telecommunication system but does not include the contents of the communication itself, contents of e-mails or interactions with websites. In this guide "data", in relation to a postal item, means anything written on the outside of the item.

3. Collateral Intrusion

Collateral intrusion is an integral part of the decision making process and should be assessed and considered very carefully by both applicants and Authorising Officers.

The Revised Codes state Collateral Intrusion is intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation such as neighbours or other members of the subject's family. Where possible, steps should be taken to mitigate collateral intrusion.

Where such collateral intrusion is unavoidable, the activities may still be authorised, provided this intrusion is considered proportionate to what is sought to be achieved. The same proportionality tests apply to the likelihood of collateral intrusion as to intrusion into the privacy of the intended subject of the surveillance.

Prior to and during any authorised RIPA activity, the RIPA authorisation and reviews should identify the likely intrusion into the subject and any collateral intrusion. Officers should take continuing precautions to minimise the intrusion where possible. The collateral intrusion, the reason why it is unavoidable and your precautions to minimise it will have to be detailed on the application and review forms. These will be considered by the Authorising Officer.

Before authorising surveillance the Authorising Officer should take into account the risk of collateral intrusion detailed on the relevant application forms as it has a direct bearing on the decision regarding proportionality.

The possibility of Collateral Intrusion does not mean that the authorisation should not be granted, but you should weigh up the importance of the activity to be carried out in operational terms on the one hand and the risk of collateral intrusion on the other hand.

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: Any authorisation for directed surveillance or CHIS will require the authorisation of the Chief Executive (or in his/her absence the Deputy Chief Executive) if it is likely that Confidential Material will be obtained.

NB Legal consultations are treated as intrusive surveillance which is outside the remit of this authority

5. 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".

6. 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"

(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).

7. 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 Part II of the RIPA 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.

8. Intrusive Surveillance

THIS CANNOT BE UNDERTAKEN BY LOCAL AUTHORITIES

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."**

Therefore, to be intrusive it has to take place actually on the residential premises or in the private vehicle except (in both cases) if a surveillance device is used. Surveillance using a device which is not on the private premises or in a private vehicle can still be "intrusive" if it consistently provides information of the same quality and detail as might be expected from a device placed on the private premises or in the private vehicle. Attaching or placing a tracking device onto, or remotely obtaining information about the location of, property without the consent of the owner and when the property is not owned by the Council is interference with property and will require a property interference authorisation from the Police, as appropriate. However, a property interference authorisation will not be required in relation to a tracking device or surveillance equipment placed on a Council vehicle to obtain information about its location.

9. Necessary

In order for an authorising Officer to decide whether an authorisation is necessary it must fall within the ground set out in Section 28(3)(b) of the RIPA. That is it must be for the purpose of preventing or detecting crime (offences referred to in paragraph A4 above) and the authorising officer must be satisfied that it is necessary to use covert surveillance in the investigation.

10. Private Information

This is defined in RIPA as including, "in relation to a person", any information relating to his or her private or family life. Private information should be taken generally to include any aspect of a person's private or personal relationship with others, including family and professional or business relationships.

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.

11. 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.

12. Proportionate

There is no strict definition but in order for surveillance or use of CHIS to be proportionate, it must not be used in cases where other more open methods of investigation will suffice. Perhaps a short period of surveillance could be justified on the grounds that it would be a quicker and easier way of obtaining evidence. Such methods must also only be used in cases where they are likely to result in the gathering of cogent evidence. The subject's situation and any known history should also be taken into account and the seriousness of the offence. 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. The authorising officer should ask him/herself:

(a) Is the use of covert surveillance proportionate to the mischief being investigated?

(b) Is the covert surveillance proportionate to the intrusion on the target and others who may be caught by it?

(c) Are there no other overt means of obtaining the information that is being sought?

13. 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.

14. Serious Crime

This is defined in section 81 subsection (3) of RIPA as crime that (a) the offence or one of the offences that is or would be constituted by the conduct is an offence for which a person who had attained the age of 21 and has no previous convictions could reasonably be expected to be sentenced to an imprisonment for a term of three years or more. (b) The conduct involves the use of violence, results in substantial financial gain or is conduct by a large number of persons in pursuit of a common purpose.

15. Subjects

A member of the public or group thereof in respect of whom surveillance, the use of a CHIS or the accessing of communications data 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, the use of a CHIS or the or accessing of communications data.

16. 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.

17. 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.

18. Senior Responsible Officer

Wigan Borough Council's Senior Responsible Officer (SRO) is the Director Resources and Contracts – Deputy Chief Executive. In accordance with the Codes of Practice, the SRO is responsible for the following areas:

a) The integrity of the process in place within the Council for the management of Covert Human Intelligence Sources and Directed Surveillance
b) Compliance with Part II of RIPA and the Codes of Practice
c) Oversight of the reporting of errors to the relevant oversight commissioner
d) Engagement with the Commissioners and inspectors when they conduct their inspections
e) Ensuring that all Authorising Officers are of an appropriate standard in light of any recommendations in the inspection reports by the IPCO
f) Reviewing and maintaining an auditable record of decisions and actions when it is decided to use covert surveillance without the protection of RIPA.

19. RIPA Monitoring Officer

Wigan Borough Council's RIPA Monitoring Officer is the Strategic Lawyer – Resources. The RIPA Monitoring Officer:

- Will maintain a central record of all original RIPA authorisations, renewals and cancellations in wet copy format.
- Will ensure that all authorisations for the use of directed surveillance have been authorised by a Magistrate as soon as practicable following approval by an authorising officer;
- Will review the authorisations/renewals made on a regular basis to ensure that such authorisations/cancellations are made properly, are appropriate and that all forms have been fully completed.
- Will also raise RIPA awareness within the Council.
- Will be prepared to advise, train and assist the Council's officers to enable them to comply with RIPA 2000.

C. SOCIAL MEDIA AND ONLINE CONTENT

1. The growth of the internet and the extent of the information that is now available online presents new opportunities for the Council to gather information which may assist them in preventing or detecting crime or carrying out other statutory functions as well as understanding and engaging with the public that they serve. It is important that the Council is able to make full and lawful use of this information for their statutory purposes. Often use of the internet prior to investigation will not engage privacy consideration but if necessary RIPA authorisations need to be considered.

2. It is not expected that a non-regular visiting or monitoring of activity on social media sites will amount to surveillance. However, planned or regular visiting or monitoring will amount to surveillance. If so, this Guide must be followed. The Home Office Codes of Practice on Covert Surveillance and CHIS also contain essential guidance in relation to online covert activity and must be consulted. This can be found at Covert surveillance and covert human intelligence sources codes of practice - GOV.UK (www.gov.uk). Paragraphs 3.10 to 3.17 of the Covert Surveillance and Property Interference Revised Code of Practice set out in detail the considerations to be worked through in order to establish whether a RIPA authorisation is necessary for any covert online investigation. Guidance on non – RIPA surveillance is at Paragraph H of this guidance

3. Care must be taken by Officers to understand how the social media site being used works. Officers must not use their personal devices or their personal social media profiles in the course of an investigation. All such investigation must take place using WBC devices and generic profiles.

4. Only publicly viewable information can be scrutinised. Officers must not attempt to view privately set information on social networking sites. Officers must not 'add' or 'follow' an investigation subject in order to access private information.

5. Further guidance relating to how information gathered from social media should be recorded can be found below at section E.

D. AUTHORISATIONS

1. Application

The whole of this section applies to directed surveillance (see definition B6 above) and the use of a CHIS (see definition B5 above). When completing an application for directed surveillance or use of a CHIS, and when completing a review, renewal and cancellation forms, regard should be had to the Council's Practical Guide to Completing the Standard Home Office Forms for Undertaking Surveillance.

2. Authorisations

Authorisations or renewals of authorisations must be given by the Authorising Officer (see definition B1 above) in writing. The Authorising Officer should forward a scanned copy of the hand signed authorisation by email immediately to the RIPA Monitoring Officer and should also forward the original authorisation to him. The RIPA Monitoring Officer will inform the Authorising Officer of the unique reference number (URN) that has been allocated to that authorisation. The URN must be included on all future review, renewal or cancellation forms in relation to that authorisation. Surveillance cannot commence until the authorised application has been considered and granted by a Magistrate.

3. Requirements

Before giving authorisation for surveillance, the use of a CHIS or the accessing of communications data the Authorising Officer must be satisfied that

(a) it is necessary for the purpose of preventing or detecting crime (offences referred to in paragraph A4 above). The written authorisation should specify the objectives of the activity in factual terms, for example, to gather evidence. The type of crime must also be specified and what facts led the Authorising Officer to believe that the activity will achieve its objectives;

(b) it is necessary in that particular case, i.e. that particular case merits the use of this method of detection over other more open methods e.g. 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 B11 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) they have considered the degree of intrusion on the targets and others within their assessment and overt measures have been considered.

NB: In cases where it is likely that knowledge of confidential information will be required authorisation will be required from the Chief Executive or the Deputy Chief Executive. In this instance approval will only be granted in exceptional and compelling circumstances.

4. The Requirement for Magistrates Approval

An authorisation, or renewal, does not commence until it has been approved by a Magistrate. A copy of the Magistrates Order approving the authorisation, or renewal, must be forwarded by email immediately to the RIPA Monitoring Officer

5. Time Limits

Written authorisations or renewals last three months beginning with the day upon which the judicial approval is obtained or renewal takes effect. The length of time for surveillance or use of a CHIS to continue should be taken into account when deciding if it is proportionate or not. Authorisation for the use of directed surveillance shall not last for more than 3 months, unless the authorisation has been renewed. Authorisations for the use and conduct of a CHIS last for 12 months (unless the CHIS is under the age of 18 years, or is a vulnerable individual, in which case the authorisation shall last for 4 months). Authorisations/notices in relation to the accessing of communications data shall not last for more than 1 month.

6. Authorising Officer

The Authorising Officer of the necessary standing in relation to the surveillance, the use of a CHIS or the accessing of communications data must be appointed by the Senior Responsible Officer and the names of such officers must be kept on records held by the RIPA Monitoring Officer.

7. Reviews

Regular reviews of authorisations must be undertaken to assess the need for the surveillance to continue. The Authorising Officer must determine how often a review should take place. Reviews should be undertaken by an authorising officer as frequently as s/he considers necessary and practicable. Bearing in mind the intrusive nature of surveillance the presumption must be in favour of early reviews. In any event a review must take place no later than one month after the date of the authorisation/renewal or last review.

There is no requirement for a Magistrate to consider the review form.

Good practice suggests that a review should ideally be carried out after the first two sets of observations to determine if the allegation being investigated has been substantiated or seriously undermined. 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.

A review form should also be submitted to record changes in circumstances during the operation so that the Authorising Officer can have the opportunity to re-evaluate the operation in question. If however there are considerable changes to the nature of the operation in question to the techniques to be used during the operation then a new application should be issued and approval sought from the Magistrates

8. Renewals

Renewals for either Directed Surveillance or CHIS application/ authorisation must be approved by a Magistrate following authorisation from the Authorising Officer.

It is important to note that the renewal must be generated before the expiry of an authorisation but such applications should not be made until shortly before the expiry of the original authorisation period is due to expire.

Authorising Officers should examine the circumstances with regard to Necessity, Proportionality and the Collateral Intrusions issues before making a decision to renew the activity. A CHIS application should not be renewed unless a thorough review has been carried out covering the use made of the source, the tasks given to them and information obtained. The Authorising Officer must consider the results of the review when deciding whether to renew or not. The review and the consideration must be documented.

In the event that the renewal envisages broadening the investigation a fresh authorisation is likely to be required. This will include situations in which suspects are added or the original authorisation is significantly different to the current activity.

9. Cancellation

The Authorising Officer must cancel an authorisation as soon as he or she believes that the activity is no longer necessary or proportionate.

The Authorising Officer must formally instruct the investigating officer to cease the surveillance. The authorising officer should record the amount of time spent on the surveillance.

All authorised applications must be cancelled as they do not naturally expire at the end of the authorisation period. It is a requirement that all those taking part in the

surveillance and/or CHIS are promptly notified of the cancellation and a record of these communications must be kept by the Authorising Officer.

Cancellation - Information required

The Authorising Officer should examine the evidence that has been obtained and check for any errors. It is also his responsibility to take the following action:

- Record dates and times that surveillance took place and the reason for the cancellation
- Ensure that the equipment has been removed and returned
- Provide directions for the management of the product
- Ensure that the detail of the property interfered with, or persons subject to surveillance since the last review or renewal is properly recorded.
- Ensure that all unauthorised activity is recorded and reported to the Commissioner forthwith in writing via the Senior Responsible Officer.
- Record the value of the surveillance (i.e. whether the objectives as set out in the authorisation were met)
- Record the current location of any equipment that has been used in connection with the surveillance.

10. Contents of Authorisation

The written authorisation should specify -

(1) names (where known) or descriptions of the subjects and any known history and character thereof;

(2) 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 equipment to be used;

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

(5) that the surveillance is necessary for the purpose of preventing or detecting crime and that it fulfils the statutory legal requirements as detailed above;

(6) that it is proportionate (see definition B11 above) i.e. specifying:

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

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

(c) why surveillance, the use of a CHIS or the accessing of communications data should be used in preference to other methods of investigation, for example it may be that it would be a means of obtaining the best evidence or the evidence could be obtained more quickly by surveillance, the use of a CHIS or the accessing of communications data than by other means;

(d) 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;

(7) The objectives of the activities;

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

(9) The length of time which should be proportionate to the wrong being investigated; and

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

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

11. Change in circumstances regarding the subject of surveillance

Authorisations should cover all known or reasonably forseeable eventualities. Accordingly if the subjectof the surveillance is likely to move the authorisation should specify this. If a subject is accompanied by, or living with, another person then the authorisation should include that other person if necessary.

12. Covert Human Intelligence Sources (CHIS's)

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 CHIS's security and welfare (the 'Handler');

(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 (the 'Controller');

(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 CHIS's is not to be disclosed unless there is a need to do so. The person responsible for maintaining a record should be an authorising officer.

A CHIS could be an informant or an undercover officer carrying out covert enquiries on behalf of the council. However the provisions of the 2000 Act are not intended to apply in circumstances where members of the public volunteer information to the Council as part of their normal civic duties, or to contact numbers set up to receive information such as the Benefit Fraud Hot Line. Members of the public acting in this way would not generally be regarded as **a CHIS**

Under section 26(8) of the 2000 Act a person is a **CHIS** if:

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

By virtue of section 26(9)(b) of the 2000 Act a purpose is covert, in relation to the establishment or maintenance of a personal or other relationship, if and only if, the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose.

By virtue of section 26(9)(c) of the 2000 Act a relationship is used covertly, and information obtained as above is disclosed covertly, if and only if it is used or, as the case may be, disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question.

13. Conduct and Use of a Source

The **use of a source** involves inducing, asking or assisting a person to engage in the conduct of a source or to obtain information by means of the conduct of such a source.

The **conduct of a source** is any conduct falling within section 29(4) of the 2000 Act, or which is incidental to anything falling within section 29(4) of the 2000 Act.

The **use of a source** is what the Authority does in connection with the source and the **conduct** is what a source does to fulfil whatever tasks are given to them or which is incidental to it. **The Use and Conduct require separate consideration before authorisation.**

When completing applications for the use of a CHIS you are stating who the CHIS is, what they can do and for which purpose

When determining whether a CHIS authorisation is required consideration should be given to the covert relationship between the parties and the purposes mentioned in a, b, and c above.

14. Management of Sources

Within the provisions there has to be;

(a) a person who has the day to day responsibility for dealing with the source and for the source's security and welfare **(Handler)**
(b) at all times there will be another person who will have general oversight of the use made of the source **(Controller)**
(c) at all times there will be a person who will have responsibility for maintaining a record of the use made of the source

The **Handler** will have day to day responsibility for:

1. dealing with the source on behalf of the authority concerned;
2. directing the day to day activities of the source;
3. recording the information supplied by the source; and
4. monitoring the source's security and welfare.

15. Tasking

Tasking is the assignment given to the source by the Handler or Controller by, asking him to obtain information, to provide access to information or to otherwise act, incidentally, for the benefit of the relevant public authority. Authorisation for the use or conduct of a source is required prior to any tasking where such tasking requires the source to establish or maintain a personal or other relationship for a covert purpose.

In some instances, the tasking given to a person will not require the source to establish a personal or other relationship for a covert purpose. For example a source may be tasked with finding out purely factual information about the layout of commercial premises. Alternatively, a Council Officer may be involved in the test purchase of items which have been labelled misleadingly or are unfit for consumption. In such cases, it is for the Council to determine where, and in what circumstances, such activity may require authorisation.

Should a CHIS authority be required all of the staff involved in the process should make themselves fully aware of all of the aspects relating to tasking contained within the CHIS codes of Practice

16. Management Responsibility

Wigan Borough Council will ensure that arrangements are in place for the proper oversight and management of sources including appointing a Handler and Controller for each source prior to a CHIS authorisation.

The Handler of the source will usually be of a rank or position below that of the Authorising Officer.

It is envisaged that the use of a CHIS will be infrequent. Should a CHIS application be necessary the CHIS Codes of Practice should be consulted to ensure that the Council can meet its management responsibilities.

17. Security and Welfare

The Council has a responsibility for the safety and welfare of the source and for the consequences to others of any tasks given to the source. Before authorising the use

or conduct of a source, the Authorising Officer should ensure that a risk assessment is carried out to determine the risk to the source of any tasking and the likely consequences should the role of the source become known. The ongoing security and welfare of the source, after the cancellation of the authorisation, should also be considered at the outset.

18. Records Relating to the CHIS

These must contain 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 (ie 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 (ie 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 WBC and allocated this task);

(h) the identities of the authorising officer and the applicant;

(i) 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

19. Accessing Communications Data

Before considering submitting an application for the acquisition of communications data, all officers must first refer the matter to the senior responsible officer or the RIPA Monitoring Officer. Communications Data ('CD') is the 'who', 'when' and 'where' of a communication, but not the 'what' (i.e. the content of what was said or written). The Council is not permitted to intercept the content of any person's communications.

Previously the Council was limited to obtaining subscriber details (known now as "entity" data) such as the registered user of a telephone number or email address. However, under Part 3 the IPA, the Council can now also obtain details of in and out call data, and cell site location. This information identifies who a criminal suspect is in communication with and whereabouts the suspect was when they made or received a call, or the location from which they were using an Internet service. This additional data is defined as "events" data.

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

The IPA has also removed the necessity for local authorities to seek the endorsement of a Justice of the Peace when seeking to acquire CD. All such applications must now be processed through NAFN and will be considered for approval by the independent Office of Communication Data Authorisation (OCDA). Applicant Officers and Authorising Officers should have regard to NAFN's User Guide and Procedures.

E. RECORDS

1. **A copy of all written authorisations, renewals, reviews, cancellations and Magistrates Orders must be forwarded by email immediately to the RIPA Monitoring Officer, Town Hall, Library Street, Wigan WN1 1YN**. The original documentation must also be sent by secure means as soon as possible to the RIPA Monitoring Officer. A copy of each form should be placed on your electronic file.

2. All written authorisations, renewals, reviews and cancellations should be kept for a period of 5 years after the conclusion of any Court proceedings arising for which the surveillance, use of the CHIS or accessing of communications data was relevant or until the next visit by theIPCO Inspectors whichever is the later. In addition, copies of such records should be retained until 5 years after any IPCO inspection. The Authorising Officer shall be responsible for the management , retention and deletion of records held by their team .The RIPA Monitoring Officer will retain oversight of the Central Record and appropriate retention and deletion procedures.

3. Where material is obtained during the course of an investigation which might be relevant to that investigation, or another investigation, or to pending or future civil or criminal proceedings, then it should not be destroyed, but recorded and retained in such a way to enable compliance with data retention and disposal. The material should be clearly labelled and stored by the relevant department. In a criminal investigation, information obtained should be recorded by means of a surveillance log. A surveillance log is a form that can be used to record an account of events observed and conversations heard at particular times.

4. .

5. All reviews of authorisations must be done in writing and kept as in E1 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.

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 3 above.

8. Such records referred to in 6. above which also reveal the name(s) of the CHIS should only be disclosed if legally necessary or if desired by any Court.

9. The Senior Responsible Officer will approve the policy on an annual basis and the Confident Council Scrutiny Committee can ensure that the revisions that have been included are fit for purpose.

10. The Confident Council Scrutiny Committee should review the authority's use of RIPA and ensure that the policy is fit for purpose at least once a year. The information will include a tabular summary setting out the essential details and outcomes of all applications. The Councillors should not, however be involved in making decisions on specific authorisations. There is a requirement that the identity of any subjects of authorised surveillance should not be identifiable in material reported to Elected Members.

11.

12. The Central Record of authorisations is held in electronically within Legal Services and is overseen by the RIPA Monitoring Officer. The Central Record should be regularly updated whenever an authorisation is granted, renewed or cancelled. It should contain the following information:

- the type of authorisation;
- the date the authorisation was given;
- the name and grade of the authorising officer
- the unique reference number (URN) of the investigation or operation;

- the title of the investigation or operation, including a brief description and names of subjects, if known;

- whether the urgency provisions were used, and if so why

- details of attendances at the magistrates' court to include the date of attendances at court, the determining magistrate, the decision of the court and the time and date of that decision

- if the authorisation has been renewed, when it was renewed and the court authorising the renewal;

- whether the investigation or operation is likely to result in obtaining confidential information as defined in the code of practice;

- whether the *authorisation* was granted by an individual directly involved in the investigation

- the date the authorisation was cancelled.

13. The following documentation should also be centrally retrievable for at least 5 years from the ending of each authorisation:

    - a copy of the application and a copy of the authorisation together with any supplementary documentation and notification of the approval given by the magistrates court;

    - a record of the period over which the surveillance has taken place;

    - the frequency of reviews prescribed by the authorising officer;

    - a record of the result of each review of the authorisation;

    - a copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;

    - the date and time when any instruction to cease surveillance was given;

    - the date and time when any other instruction was given by the authorising officer

14. Destruction

    Information obtained through 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). If such information is retained, it should be reviewed at appropriate regular intervals to confirm that the justification for its retention is still valid.

F. <u>COMPLAINTS</u>

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

G. FORMS

All forms used to apply for, review, renew or cancel authorisations under RIPA shall be in the form approved by the Home Office and can be found at the following internet address:

http://www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/ripa-forms/

Regard should be had to the Council's Practical Guide to Completing the Standard Home Office Forms for Undertaking Surveillance when the forms are being completed

H. NON-RIPA SURVEILLANCE

On occasion, the Council may undertake surveillance which does not meet the criteria to use the RIPA legislation. However, the Council must still meet its obligations under the Human Rights Act and therefore any surveillance outside of RIPA must be necessary and proportionate.

There may be occasions when covert or direct surveillance specifically focuses attention on an individual whether for purposes of an investigation or operation conducted by Wigan Council. The individual will not be aware of the surveillance and the surveillance is aimed at obtaining evidence as part of an investigation.

The main principles are that those undertaking such surveillance should ensure that the Human Rights Act rights to a private life are not breached. Therefore, the surveillance should be both necessary and proportionate. The definition of necessary and proportionate is included in the Definitions (Para B) of this procedural guide.

It is important to consider not just the privacy of the person who is the subject of the investigation but any third party that may be affected as a result of that surveillance. It is necessary to avoid intrusion on third parties and minimise any necessary intrusion into the lives of those not directly connected with the investigation of operation procedures.

The authorising officer will objectively have to satisfy themselves whether or not the use is proportionate and necessary and whether it should be authorised.

In doing so authorising officers must pay particular attention to the following issues:

(1) Data Protection considerations.

(2) Health and Safety considerations.

(3) Resource implications.

(4) The principles of the Human Rights Act and the need to respect family life and privacy.

The authorising officer must ensure that they complete the attached form and keep an accurate record which should be submitted to the RIPA Officer for the Council who is Janet Davies, Strategic Lawyer - Resources. Any non-RIPA surveillance must operate for a fixed time and as a matter of good practice its use should be reviewed every 6 weeks. The application form should be completed by the originating officer and then signed by the authorising officer. Any granted authorisations will be kept alongside the RIPA authorisation records and will contain a copy of the application form, the authorisation and the review papers.

For more information Contact the RIPA Monitoring Officer:

Janet Davies
Strategic Lawyer - Resources
Resources Directorate
Legal Division
Town Hall, Library Street, Wigan WN1 1YN
Tel. 01942 827028 (Internal Ext. 2028)
Email: janet.davies@wigan.gov.uk