Welwyn Hatfield Council
Regulation of Investigatory Powers Act 2000
As amended by the Protection of Freedoms Act 2012

1. Introduction

The Council is committed to working for the overall good of the people of Welwyn Hatfield. In carrying out its duties the Council may need to conduct appropriate investigations into allegations or concerns brought to its attention. Occasionally, our investigations will require us to gather information in respect of individuals who may be unaware of what we are doing (through covert surveillance). In conducting our investigations we need to draw a fair balance between the public interest and the rights of individuals. In order to achieve that balance, the Council will take into account and comply with the Regulation of Investigatory Powers Act 2000 (RIPA) (as amended) and the Human Rights Act 1998. This policy therefore sets out the Council's approach to covert surveillance issues falling within the framework of RIPA in order to ensure consistency, balance and fairness. This information will provide additional protection and safeguards where these covert activities are likely to cause us to obtain what is termed "Private information" about individuals or where we go "under cover" in certain circumstances. This policy also makes it clear to the general public what checks and balances will apply.

The purpose of this policy is to provide guidance and a framework for the Council's activities under the Act in relation to their specific public functions.

The Office of the Surveillance Commissioners (OSC) both advises the Council and members of the Public about these issues and the OSC also periodically audits and inspects the way in which Local Authorities including the Council work in accordance with the Act. The Council was last inspected in February 2016 and received a favourable report.

The Protection of Freedoms Act 2012 amended RIPA to make local authority authorisations subject to judicial approval. The change means that the Council need to obtain an order approving the grant or renewal of an authorisation from a judicial authority, before it can take effect. An application for such an order must be made to a Justice of the Peace (JP) also known as a Magistrate. If the JP is satisfied that the statutory tests have been met and that the use of the technique is necessary and proportionate, he or she will issue an order approving the grant or renewal for the use of the technique described in the application. The amendment means that the Council is no longer able to orally authorise the use of RIPA techniques. All authorisations must be made in writing and require JP approval. The authorisation cannot commence until this has been obtained and the activity must be carried out in accordance with that authorisation.

2. Definitions

The essential key to understanding the way that RIPA works is to understand the definitions used within it. Awareness as to whether a proposed action comes within RIPA is critical in establishing whether authorisation needs to be sought, if any and at what level.

There are three categories of covert activity:

a) **Intrusive surveillance** – This is covert and carried out in relation to anything taking place on any residential premises or any private vehicle. It involves a person on the premises or in the vehicle or is carried out by a surveillance device. Except in cases of emergency, it requires OSC approval. The power is available only to Law enforcement agencies. **Intrusive surveillance cannot be undertaken by the Council.**

b) **Directed surveillance** - This is covert surveillance but not intrusive surveillance. It is undertaken for a specific investigation or operation in a way likely to obtain private information about an individual. It must be necessary and proportionate to what it seeks to achieve. It may be used by a wide range of authorities identified in the legislation including the Council.

   Local authorities in England & 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 six months imprisonment or are related to the underage sale of alcohol and tobacco. 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 six months imprisonment.

   Local authorities may therefore continue to authorise the use of directed surveillance in more serious cases as long as they are satisfied that it is necessary and proportionate and prior approval of a JP has been granted. Examples would include more serious criminal damage, dangerous waste dumping and serious or serial benefit fraud.

   A local authority MAY NOT AUTHORISE the use of directed surveillance under RIPA to investigate disorder that does not involve criminal offences or to investigate low level offences for example, littering, dog control and fly-posting.

CCTV and automatic number plate recognition (ANPR) cameras

The use of overt CCTV cameras by public authorities does not normally require an authorisation under the Act. Similarly, the overt use of ANPR systems to monitor traffic flows or detect motoring offences does not require an authorisation.

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

Online covert activity

The use of the internet may be required to gather information prior to and /or during an operation, which may amount to directed surveillance. Whenever a public authority intends to use the internet as part of an investigation, they must first consider whether the proposed activity is likely to interfere with a person's Article 8 rights, including the effect of any collateral intrusion. Any activity likely to interfere with an individual's Article 8 rights should only be used when necessary and proportionate to meet the objectives of a specific case. Where it is considered that private information is likely to be obtained, an authorisation must be sought as set out in this policy. Where an investigator may need to communicate covertly online for example for contacting individuals using social media websites, a CHIS authorisation should be considered.

c) **Covert human intelligence sources –** Known as CHIS. This is the use or conduct of someone "undercover" that establishes or maintains a personal or other relationship with a surveillance subject for the covert purpose of obtaining information. An Authorising Officer must be satisfied that the CHIS is necessary, that the conduct authorised is proportionate to what is sought to be achieved and that arrangements for the overall management and control of the undercover officer are in force. CHIS may be used by a wide range of authorities identified in the legislation again including the Council. CHIS authorisations will not normally be granted owing to the threshold test of necessary and proportionality .

It is legally possible for councils to also undertake elementary communications interception, but in reality (and on advice from

inspecting officers) like CHIS the Council does not see this tool as relevant to our investigatory work.

Other definitions which can be usefully explained are:

d) Overt surveillance – to paraphrase the legal definition, this covers all situations where surveillance is not covert. Overt surveillance does not require authorisation under RIPA.

e) Surveillance – The monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications or recording anything monitored, observed or listened to in the course of surveillance and includes surveillance by or with the assistance of a surveillance device i.e. Camera, Video Recorder.

f) Private information needs to be interpreted in line with the European Court for Human Rights explanation of private life which includes business and professional activities

3. Codes of Practice

Whilst this policy is intended to provide an overview of RIPA and its relevance to this Council, detailed codes of practice are available from the Home Office. Officers likely to conduct surveillance and Authorising Officers should ensure they are familiar with these codes. The codes are not themselves law but they are statutory guidance, citable in a court of law and any deviation from them will require to be justified. Failure to comply with the code carries the risk that valuable and often critical evidence may be ruled inadmissible by courts. It is suggested that all relevant staff should be aware of these codes which can be found on the Home Office website at http://www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/ripa-forms/

Electronic versions of the application forms can also be downloaded from this site. Investigating officers are responsible for ensuring that they are using the most up to date forms.

4. Conducting covert surveillance and using CHIS in accordance with the Act.

It is the responsibility of the investigating officer/case officer to determine if surveillance techniques may be appropriate to aid investigation. They should have early discussions with a RIPA authorising officer to ascertain if RIPA authority is required. Where a RIPA authority cannot be issued then the case officer is responsible for ensuring that overt surveillance

techniques are used or that no surveillance takes place. It is council policy that covert surveillance will only take place with a RIPA authority in place.

In determining whether a RIPA authority is required the case officer will need to explain to the authorising officer whether the offence which is under investigation:

a) Carries a minimum tariff of at least 6 months imprisonment
   or
b) Is a specified offence relating to the sale of alcohol
   or
c) Is a specified offence relating to the sale of tobacco
d) And that covert surveillance is necessary and proportionate to the matter under investigation
e) And that there are no alternative means of obtaining the evidence

A RIPA authority can only be considered in regard to the prevention of crime relating to the above offences (or for disorder if it also meets one of the above definitions). Blanket authorisations covering “crime and disorder” are not allowed.

Once it has been decided that there is a need for covert surveillance or an undercover exercise, express authorisation needs to be obtained. The case officer will need to complete the relevant parts of the authorisation form and the Council will have appropriately trained officers who will need to complete the authorising officers statement on the forms depending on the activity sought to be authorised. The case officer and authorising officer must make sure they show why the surveillance is necessary and proportionate on the form. Sufficient detailed information must be provided, including for example the “who, what, when, where and hows” of the authorisation. It must be clear as to who has been authorised to do what, when they can carry it out and how they are to undertake the surveillance.

The Council currently have Four trained officers who may authorise investigations. (Authorising Officers) These are: (see also note below regarding confidential information)

- Nick Long – Corporate Director (Public Protection, Planning and Governance) and Senior Responsible Officer
  01707 357401 n.long@welhat.gov.uk
- Joanna Harding – Head of Public Health and Protection
  01707 357361 jo.harding @welhat.gov.uk
- Ian Colyer – Principal Governance Officer
  01707 357413 i.colyer@welhat.gov.uk
- Kate Payne, Licensing Team Leader
  01707 357206 k.payne@welhat.gov.uk

In general authorisation should be sought punctually and in advance of the activity constituting the covert surveillance or use of CHIS. Wherever possible the circumstances of the case should be discussed with the authorising officer in order for a reasoned decision as to whether surveillance or CHIS is necessary and whether alternative means of obtaining information has been considered.

In cases where through the use of surveillance it is likely that confidential information will be acquired, the use of surveillance is subject to a higher level of authorisation. This responsibility cannot be delegated. The code of practice sets out the required level of authorisation for local authorities as the Head of Paid Service (At Welwyn Hatfield this is the Chief Executive) or in his absence a Director acting as Head of Paid Service. Confidential information consists of:

- Matters subject to legal privilege as described in section 98 of the Police Act 1997.
- Personal information being information held in confidence concerning an individual (living or dead) who can be identified from it and who can be identified from it and relating to physical or mental health, spiritual counselling or other assistance or information which a person has acquired or created in the course of any trade, business, occupation or for the purposes of any paid or unpaid office.
- Confidential journalistic information which includes information acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence.

It should be noted that recent changes to the legislation brought about by the Protection of Freedoms Act 2012 mean that an authorisation for surveillance can only be brought into effect once it has been approved by a JP/Magistrate. Application for such approval must only take place once one of the council's appointed authorising officers has signed off the application for surveillance.

The case officer and authorising officer will need to attend court having completed the necessary court application form and telephoned the court in advance to arrange a hearing. It is generally not good practice or appropriate to just turn up at the court house without prior agreement.

The JP/Magistrate will perform a paperwork review and this is why it is important that all relevant material is contained in the RIPA application. It will not be possible to introduce any additional evidence outside the content of the RIPA form.

The JP/Magistrate may grant the application, may choose to refuse it (in which case amendments can be made and a new application submitted) or quash the application.

A RIPA application authorised by a local authority cannot take effect until judicial approval has been given. This may be different to other agencies who use RIPA so care must be taken when running joint operations.

The council's legal team will arrange for access to a JP/Magistrate and in exceptional circumstances this could be arranged out of hours/outside of a court location.

5. Undertaking surveillance

Investigating officers of the Council should bear in mind the following:

- Covert surveillance or CHIS should only be undertaken for as long as it is needed for the purpose for which it is authorised. Surveillance should not be undertaken for longer periods than absolutely necessary. In short, surveillance should only be undertaken for as long as it is required to obtain the necessary information.
- Officers should seek to reduce any collateral intrusion into the lives and business of the subject and also the subject's family, colleagues or associated third parties.
- The amount of private information received during the course of surveillance should be kept to a minimum.
- Adequate safety and welfare checks have been carried out prior to the use of CHIS. Where the CHIS is not an employee of the Council or has not received sufficient training for this work, the officer in charge of the surveillance should have put in place measures to ensure that assistance is close at hand should this be required.
- All officers should act diligently and professionally regarding their own and colleagues safety and the safety of any surveillance equipment at their disposal.

6. Surveillance equipment

Council officers conducting surveillance must endeavour to use equipment at their disposal in a responsible and discrete manner. Officers should be aware that the use of any equipment is restricted to being used in a manner that constitutes covert surveillance only. If there is a risk that the use of such equipment will transform the operation into an intrusive one then the surveillance should cease immediately.

Upon the cessation of surveillance officers should ensure that any equipment is properly checked upon its return to storage. This should include condition and to ensure that material that could fall into the possession of unauthorised staff is removed. An example of this is the removal of video tapes that may contain images used for evidence.

If any faults are detected with the equipment this should be brought to the attention of the authorising officer as soon as possible. Under no circumstances should the authorising officer seek to rectify any faults as

this could affect the admissibility of the evidence contained on the equipment or obtained by using it.

7. Authorising Officers

When deciding whether or not authorisation is warranted in a particular circumstance the Authorising Officer has to ask three relevant questions:

a. Is the surveillance for a relevant offence?

b. Is the surveillance necessary for the purpose of preventing or detecting crime or preventing disorder? In this context necessary means that there is no other way of obtaining the information other than by covert surveillance, i.e. all other investigatory tools and options have been exhausted or are wholly inappropriate

c. Is the conduct of the surveillance proportionate to its aim? In this context proportionality requires consideration of

- Balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence
- Explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others
- Considering whether he activity is appropriate use of the legislation in a reasonable way having considered all reasonable alternatives of obtaining the necessary result
- Evidencing as far as reasonably practicable what other methods have been considered and why they were not implemented.

In simple terms can the objective of the surveillance be important enough to justify the interference with an individual's liberty and privacy?

The Authorising Officer should also consider the means of surveillance and whether this is the most appropriate in the specific circumstances. Does it minimise intrusion into an individual's private life and is it a workable method of obtaining information?

Authorising Officers should keep the scope of the authorisation to a minimum i.e. sufficient authorisation to gather the required information but nothing more. The Investigating Officer must be made fully aware of the limits of the authorisation.

There is an automatic **Three month** restriction on the grant of any directed surveillance authorisation. Further authorisation will need to be sought for periods over this in the form of a renewal application. If a short sharp operation is envisaged then the correct procedure is to grant the authorisation for 3 months but to schedule an appropriate early review and to cancel the authorisation as soon as it is no longer necessary or proportionate.

8. Review

Whilst the initial authorisation may be valid for up to three months, if the Authorising Officer considers that a review should be carried out before this time then this should be carried out.

9. Renewals

Authorising Officers may renew applications to conduct surveillance (Including oral reviews in the case of emergencies) and renewals will last for a further three months from the date of the original authorisation terminating.

Authorising Officers should note that changes in circumstances to particular cases and any effects that such changes would have on the need for surveillance or the nature of it should be carefully considered. In all cases a note should be made on the renewal form whether it is a first or subsequent renewal.

10. Cancellation of Authorisation

Before an authorisation lapses, it must be reviewed by the Authorising Officer and cancelled where appropriate rather than letting an authorisation lapse. It is of paramount importance that all officers involved in the surveillance are made aware of the cancellation.

Officers who continue to conduct surveillance once it is brought to their attention that it is no longer authorised may be liable to disciplinary proceedings. Potential court action could also be taken against officers by any party affected by unauthorised surveillance.

11. Authorisation forms

The case officer must ensure they have the latest version of the forms. These can be obtained from the home office website.

The initial authorisation form and any renewals will be kept by the authorising officer for the duration of the authorisation. A unique reference number will be allocated by the Senior Responsible Officer.

Upon the cessation of the authorisation forms should be sent to the Council's Senior Responsible Officer for safe custody.

Forms will be stored for a period of three years from the date of the authorisation ceasing. Forms may be recalled by the Authorising Officer or by the officer applying for authorisation if for example the investigation has restarted. Any removal of forms must be accompanied by the completion of a log sheet indicating when the form was removed and by whom.
Any officer who removes forms will be responsible for the safe keeping of those forms. Disciplinary action may be taken against officers who do not comply.
Under no circumstances must the forms that have been removed be altered or amended in any way. Again disciplinary action may be taken for non-compliance.
Forms may be electronically scanned and stored for the sake of practicality.

12. General Information

This policy is a public document and is available for public inspection at the Council's main offices at Campus East, Welwyn Garden City, Hertfordshire AL8 6AE. The document is also available on the Council website at www.welhat.gov.uk
The policy will be reviewed from time to time.

13. Complaints

RIPA has established an independent Tribunal made up of senior members of the judiciary and legal profession and is independent of the Government.

Complaints by members of the public, surveillance subjects or others which relate to any aspect of surveillance carried out by Council officers will be dealt with as follows:

- The complainant will be directed to the Council's Complaint procedure and will be given a copy of the standard complaint form.
- If the complainant is still not satisfied they have the right to complain to the Investigatory Powers Tribunal, PO Box 33220, London SW1H 0ZQ Tel: 020 7035 3711 https://www.ipt-uk.com/

Additionally dependent on the nature of the complaint the complainant may also be put in touch with the Local Government and Social Care Ombudsman. https://www.lgo.org.uk/ telephone 0300 061 0614

14. Training and review.

The council will arrange for Authorising officers to receive training. Where relevant and necessary in the conduct of their jobs, Heads of Service are responsible to ensure a training programme for their staff which covers use of RIPA and authorisation requirements for covert surveillance. The Authorising Officers can assist with this training. The Authorising Officers will periodically review the corporate training needs regarding RIPA and the promotion of good surveillance practice.

15. Oversight by elected members

Elected members of a local authority should review the authority's use of RIPA and set the policy at least once a year. They should also consider internal reports on the use of RIPA on a regular basis to ensure that it is being used consistently with the local authority's policy and that the policy remains fit for purpose.

16. Record Keeping

A record of the following information pertaining to all authorisations shall be centrally retrievable within each public authority for a period of at least three years from the ending of each authorisation. At the Council this will be held by the Director (Public Protection, Planning and Governance) who is the Council's Senior Responsible Officer. This information will be regularly updated whenever an authorisation is granted, renewed or cancelled and will be made available for inspection by the relevant commissioner.

- The type of authorisation
- The date the authorisation was given
- Name and grade of the Authorising Officer
- The unique reference number of the investigation
- The title of the investigation including a brief description and names of subjects
- Details of attendances at the magistrates court to include the date of attendance at court, the determining magistrate, the decision of the court and the time and date of that decision
- The dates of any reviews
- If the authorisation has been renewed, when it was renewed and who authorised the renewal including the name and grade of the Authorising Officer
- Whether the investigation is likely to result in obtaining confidential information as defined in the code
- Whether the authorisation was granted by an individual directly involved in the investigation
- The date the authorisation was cancelled

The following documentation will also be held centrally:

- A copy of the application and a copy of the authorisation together with any supplementary documentation and notification of the approval given by the authorising officer
- A record of the period over which the surveillance has taken place
- The frequency of reviews prescribed by the Authorisation Officer
- A record of the result of each review of the authorisation
- A copy of any renewal of an authorisation together with any 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 authorisation officer
- A copy of the order approving or otherwise the grant or renewal of an authorisation from a JP/Magistrate

The Council will ensure that arrangements are in place for the secure handling, storage and destruction of material obtained through the use of directed or intrusive surveillance. Authorising Officers will be responsible for ensuring compliance with the appropriate data protection requirements under the Data Protection Act 2018 , The General Data Protection Regulations 2018 and any relevant codes of practice relating to the handling and storage of material.