Public Document Pack

WELWYN HATFIELD

Please note that by law this meeting can be filmed, audio-recorded, photographed or reported electronically by the use of social media by anyone attending. This does not apply to any part of the meeting that is held in private session.

Please ask for:
Vanisha Mistry

28 January 2022

Dear Councillor

You are requested to attend a meeting of the WELWYN HATFIELD BOROUGH COUNCIL STANDARDS COMMITTEE to be held on Monday 7 February 2022 at 7.30 pm in the Council Chamber, Campus East, Welwyn Garden City, Herts, AL8 6AE.

Yours faithfully

Governance Services Manager

A G E N D A
PART 1

1. APOLOGIES

2. MINUTES

   To confirm as a correct record the Minutes of the meeting on 20 September 2021 (Circulated separately).

3. DECLARATIONS OF INTERESTS BY MEMBERS

   To note declarations of Members' disclosable pecuniary interests, non-disclosable pecuniary interests and non-pecuniary interests in respect of items on this Agenda.

4. NOTIFICATION OF URGENT BUSINESS TO BE CONSIDERED UNDER ITEM 6

5. UPDATES TO THE REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA) POLICY AND LIST OF AGREED AUTHORISING OFFICERS (Pages 3 - 20)

   Report of the Head of Law and Administration on updates to the RIPA authorising Officers and Senior Responsible Officer (SRO) and to agree that the corporate RIPA policy is updated.

6. SUCH OTHER BUSINESS AS, IN THE OPINION OF THE CHAIR, IS OF SUFFICIENT URGENCY TO WARRANT IMMEDIATE CONSIDERATION

7. EXCLUSION OF PRESS AND PUBLIC

The Committee is asked to resolve:

That under Section 100(A) (2) and (4) of the Local Government Act 1972, the press and public be now excluded from the meeting for item 8 (if any) on the grounds that it involves the likely disclosure of confidential or exempt information as defined in Section 100A (3) and Part I of Schedule 12A of the said Act as amended.

In resolving to exclude the public in respect of the exempt information, it is considered that the public interest in maintaining the exemption outweighs the public interest in disclosing the information.

PART II

8. ANY OTHER BUSINESS OF AN EXEMPT NATURE AT THE DISCRETION OF THE CHAIR

Circulation: Councillors T.Kingsbury (Chairman), G.Michaelides, L.Musk, N.Pace, P.Zukowskyj

Co-opted Member - Representative of the Welwyn Hatfield Association of Local Councils
Parish Councillor B.Morris

Corporate Management Team
Press and Public (except Part II Items)

If you require any further information about this Agenda please contact Vanisha Mistry, Governance Services by email – democracy@welhat.gov.uk

Part I
Main author: Alison Marston
Executive Member: Cllr Nick Pace
All Wards

WELWYN HATFIELD BOROUGH COUNCIL
STANDARDS COMMITTEE - 7 FEBRUARY 2022
REPORT OF THE HEAD OF LAW AND ADMINISTRATION

UPDATES TO THE REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA) POLICY AND LIST OF AGREED AUTHORISING OFFICERS

1 Executive Summary

1.1 Following recent staff changes, Standards Committee is asked to note and agree the updates to the RIPA authorising Officers and Senior Responsible Officer (SRO) shown below and to agree that the corporate RIPA policy is updated accordingly, as shown in Appendix A.

2 Recommendation(s)

2.1 For Standards Committee to note the changes detailed in this report.

3 Explanation

3.1 The council has powers to investigate a range of criminal offences and like all Local Authorities is able to utilise powers to undertake surveillance to assist with those investigations in certain prescribed circumstances.

3.2 As previously reported to Committee the use of these powers is governed by the requirements of law and the Council's own policy. Powers cannot be used without the agreement of a designated "Authorising Officer" and the approval of a Magistrate. In all cases the powers can only be used to investigate a specified offence and must be shown to be necessary and proportionate to the circumstances.

3.3 It is timely and necessary to make a number of updates to the list of Authorising Officers, as shown below and Standards Committee are asked to agree these updates and consequential amendments to the current policy as set out in appendix A.

Senior Responsible Officer
Amended to **Head of Law and Administration – Margaret Martinus**

Authorising Officer
Removal of Corporate Director (Public Protection, Planning and Governance)

All other designations remain the same as in previous versions of the policy.

3.4 Standards Committee should also be updated on two further matters.

3.5 Firstly, that the Investigatory Powers Commissioner's Office (IPCO), the Government Regulator for the use of RIPA by enforcing authorities, annual return has been submitted by the Council and that there were no authorisations issued by the Council in the period 1st January to 31st December 2021.

3.6 Secondly, that we received our IPCO inspection on 21st January 2022. The official inspection letter confirming the findings has yet to be received by the Council. However, the inspector found everything to be operating satisfactorily and confirmed that he would be writing to the Council on this basis.

3.7 The inspector did make some suggested best practice amendments to the RIPA policy and these amendments will be made to the policy, once the formal letter has been received.

3.8 The suggested amendments were:-

-web links to the Codes of Practice should go directly to these codes.

-communications data- consider membership of the National Anti-Fraud network as they are a single point of contact for communications data.

-rationalise references to confidential data and ensure that they are all linked in the policy.

-reviews and renewals- amend to reflect Code that reviews must be carried out after three months. This is a mandatory requirement.

-suggested insertion of role that IPCO fulfils in the statutory regime, within the policy.

4 Legal Implication(s)

The Regulation of Investigatory Powers Act (RIPA), as amended by the Protection of Freedoms Act and Investigatory Powers Act 2016 sets out the regulatory regime by which the council may use certain surveillance powers to investigate certain specified offences. There are strict controls in place and the council is unable to undertake any “covert surveillance” outside of this regime. Failure to comply with the legislation could result in legal challenge or challenge on the admissibility of evidence in Court.

5 Financial Implication(s)

5.1 A training budget is in place for authorising officer training.

6 Risk Management Implications

6.1 The risks related to this proposal relate to legal challenge and reputation, for example a significant court case collapsing owing to evidence collected through surveillance being ruled inadmissible. However, there are strict controls in place to govern the approval of any surveillance authorisations and the council does not carry out covert surveillance outside of the RIPA regime. Additionally, a staff training programme is in place and Heads of Service are asked to ensure relevant staff attend the training programme. RIPA compliance is also included as part of the management assurance statements which help comprise the annual governance statement and the Council is periodically audited by the Office of Surveillance Commissioners. An assessment of risk is therefore considered as impact: high, probability: low

7 Security and Terrorism Implication(s)

7.1 The RIPA regime is used by the Council to assist with the investigation of certain criminal offences. In addition, the Council will work, as required, with the police and other partners to facilitate the prevention, detection and investigation of crime.

8 Procurement Implication(s)

8.1 None

9 Climate Change Implication(s)

9.1 None

10 Human Resources Implication(s)

10.1 As previously reported to Committee the council has a RIPA training programme in place for staff including investigation officers, officers with access to IT systems and Authorising Officers.

11 Health and Wellbeing Implication(s)

11.1 None

12 Communication and Engagement Implication(s)

12.1 The nature of any covert surveillance undertaken by the council is by definition "covert" and therefore not in the public domain. However, for public confidence and transparency it is important that the Council shares its adopted RIPA policy and once updated this policy will be republished on the Council's webpage.

13 Link to Corporate Priorities

13.1 The subject of this report is linked to the Council's Corporate Priorities "our community", "our environment", "our housing" and "our council" and the statutory provisions under the Regulation of Investigatory Powers Act (RIPA), as amended.

14 Equality and Diversity

14.1 An Equality Impact screening assessment (EQIA) has not been carried out in connection with the proposals that are set out in this report as RIPA is an enforcement tool and an EQIA was carried out in connection with the council's corporate enforcement policy which sets out our overall approaches to enforcement.

Margaret Martinus
Head of Law and Administration
RIPA Senior Responsible Officer

January 2022

Appendix A: Updated Corporate RIPA Policy

This page is intentionally left blank

Welwyn Hatfield Borough Council

Regulation of Investigatory Powers Act 2000 (RIPA) Policy

WELWYN HATFIELD

Working better, together

Table of Contents

Purpose of this policy 2
Background 2
Codes of Practice 3
Definitions 3
Council use of covert human intelligence sources (CHIS). 4
Council use of communications data 4
Council use of covert directed surveillance 4
Particular circumstances 8
Surveillance equipment 8
CCTV and automatic number plate recognition (ANPR) cameras 8
Online activities 8
Tracking devices 9
Drones and unmanned Arial vehicles (UAV) 9
Noise nuisance and similar recordings 9
Authorising Officers 10
Undertaking surveillance 10
Review and renewals 11
Cancellation of Authorisation 11
Authorisation forms 11
General Information 11
Training and review 12
Record Keeping 12
Mandatory reporting 13
Oversight by elected members 13
Complaints 13

Purpose of this policy

The council is able to investigate a variety of criminal offences, and from time to time officers of the council may need to use investigation techniques which are covered by the Regulation of Investigatory Powers Act 2000 (RIPA) (as amended by the Protection of Freedoms Act 2012 and the Investigatory Powers Act 2016).

This policy, which has been endorsed by the Full Council, sets out the council's commitment to abide by the relevant legislation, to follow the official Codes of Practice, to appropriately train employees and review its activities so that investigations are not compromised by poor practice and the public can have confidence in the council's investigatory work.

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.

Background

The Human Rights Act affords everyone an expectation of their right to privacy and whilst it may be obvious of an expectation to a right to privacy in a private place, the code of practice is clear that there could also be an expectation of a right to privacy (albeit reduced) in certain public places, including the online space (i.e. internet). RIPA provides a lawful mechanism for the council in certain very specific and controlled circumstances to breach that right.

The Council is committed to working for the overall good of the people of Welwyn Hatfield. Therefore in carrying out its duties the Council may need to conduct appropriate investigations into allegations or concerns brought to its attention. Very 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 must 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.

The Investigatory Powers Commissioner (IPC) advises the Council and members of the Public about these issues and the IPC will periodically audit and inspect the way in which Local Authorities including the Council work in accordance with the Act. The IPC has taken over from the Office of the Surveillance Commissioner (OSC) who performed a similar role. The Council was last inspected by the IPC in February 2019 and received a favourable report.

The Protection of Freedoms Act 2012 amended RIPA to make local authority authorisations subject to judicial approval. This change means that the Council needs to obtain the agreement of a Magistrate before it can undertake covert surveillance or to renew an authorisation for covert surveillance.

If the Magistrate is satisfied that the statutory tests have been met and that the use of the technique is necessary and proportionate, they will issue an order approving the grant or renewal for the use of the technique described in the application. This means that the Council is no longer able to orally authorise the use of RIPA techniques and all authorisations must be made in writing and require judicial approval. The authorisation cannot commence until this has been obtained and the activity must be carried out in accordance with that authorisation.

The requirement for judicial approval provides an additional safeguard and assurance to the public that the council will only use covert surveillance techniques where it is shown to be necessary and proportionate.

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. This policy makes it the responsibility of Officers likely to conduct surveillance, their Managers and the council's appointed Authorising Officers to ensure they have access to and are familiar with these codes and any accompanying guidance.

The codes have recently been updated and although are not themselves law they are 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 the Courts.

All relevant staff are expected to carefully read the appropriate parts of the revised codes when considering operations and preparing applications. The revised codes have been incorporated into staff training which is periodically offered to our staff involved in investigations.

The codes can be found on the Home Office website at:
http://www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/ripa-forms/
https://www.gov.uk/government/collections/ripa-forms--2

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.

Definitions

The essential key to understanding the way that RIPA works and how the council will use it, is to understand certain key definitions. Awareness as to whether a proposed action comes within RIPA is critical in establishing whether authorisation actually needs to be sought and at what level.

There are several categories of covert activity, some of which the council may potentially use. However on advice from inspecting Deputy Surveillance Commissioners and taking account of the nature and limited range of criminal offences which the council may investigate, this policy recognises that showing "necessity" and "proportionality" for some of these techniques in a council setting is unlikely and therefore the council is highly unlikely to use them. Additionally there are some activities which the council is prohibited by law from using.

Type of activity	Brief description	Notes
Directed surveillance	Covert surveillance which is not intrusive; undertaken for a specific operation in relation to a relevant offence and in a way likely to obtain private information about an individual	Council may use this
Covert Human Intelligence sources (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.	Council unlikely to use this
Communications data access	Access to data showing when particular communications took place, but not the content of those communications	Council advised not to use this
Intrusive surveillance	Covert surveillance carried out in relation to anything taking place on any residential premises or any private vehicle where it involves a person on the premises or in the vehicle or is carried out by a surveillance device.	By law the council cannot use this

Other key terms which can be usefully explained are:

Term	Brief description
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 equipment such as cameras, video recorder, binoculars or similar.
Private information	This term needs to be interpreted in line with the European Court for Human Rights explanation of private life and the latest code of practice. In essence it means private information includes any aspect of a person's private or personal relationships with others such as family, professional and business relationships.
Non private information	May include information about a person which is in the public domain such as newspapers, journals, TV broadcasts, websites and articles. It may include information only available after the payment of a fee and any data which is made available on request
Overt surveillance	To paraphrase the legal definition, this covers all situations where surveillance is not covert. It is done in the open, for example using uniformed staff, marked vehicles or public CCTV systems which scan a general area. Overt surveillance does not require authorisation under RIPA
Covert surveillance	Means surveillance carried out in such a way calculated to ensure that the person who is the subject of the surveillance is unware it is taking place, or surveillance carried out by use of a surveillance device
Confidential information	Certain information for example relating to medical records, legal privilege or journalistic sources. Only the councils Head of Paid Service (or appointed Deputy) may authorise surveillance to obtain confidential information
Collateral intrusion	Information obtained during surveillance which relates to a third party who is not the subject of the surveillance

Council use of covert human intelligence sources (CHIS).

It is considered highly unlikely that the council will ever consider the deployment of CHIS as being necessary and proportionate, and to do so the 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. These can be onerous, and CHIS authorisations will not normally be granted owing to the threshold test of necessary and proportionality and the specific skills needed to operate, handle and manage CHIS.

However as pointed out during OSC inspections, it is important that council officers are aware of what constitutes a CHIS so that they do not inadvertently create one, therefore an explanation of CHIS and associated risks is included in the training for our investigatory officers.

Council use of communications data

As noted above, 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.

Council use of covert directed surveillance

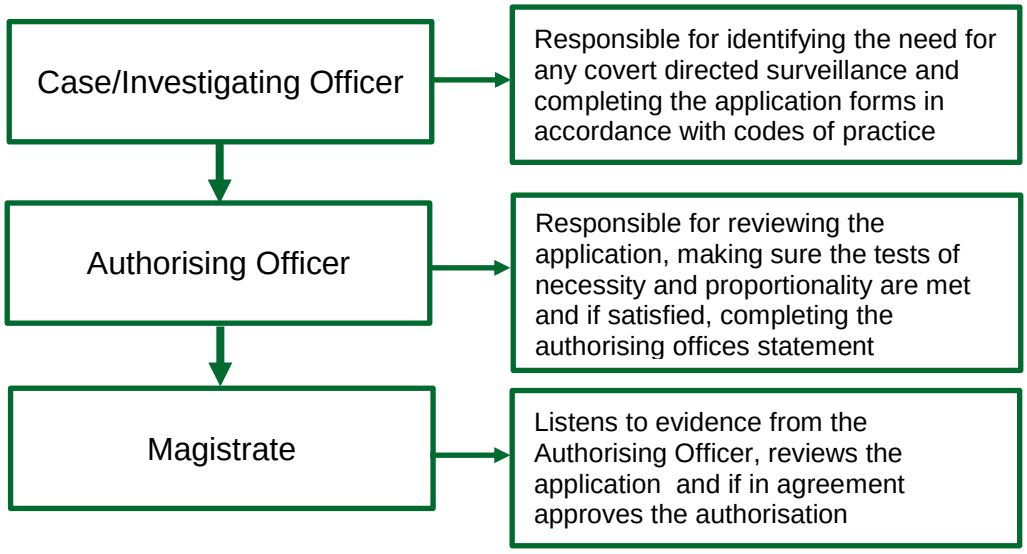
Like all Local authorities in England & Wales the council can only authorise use of directed surveillance under RIPA to prevent or detect criminal offences that are either punishable,

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.

The council may therefore 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 Magistrate has been granted. Examples would include more serious criminal damage, dangerous waste dumping and serious or serial benefit fraud.

A local authority such as the council 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.

Three separate people are involved in granting an authorisation for covert directed surveillance by the council:



It is the responsibility of the investigating officer/case officer to determine if surveillance techniques may be appropriate to aid an investigation. They should have early discussions with a RIPA authorising officer to ascertain if RIPA authority is required (a suitable flow chart is included in appendix A)

Where a RIPA authority cannot lawfully be issued then the case officer is responsible for ensuring that only overt surveillance techniques are used and that no covert surveillance takes place.

It is council policy that covert surveillance will only take place with a lawful authority in place. If no RIPA authorisation can be given, and there is no other power to carry out the covert surveillance, then it must be made overt. Ways of making surveillance overt include:

- uniformed staff,
- notification of intentions,
- marked vehicles,
- signs
- publicity and
- ensuring the surveillance is not carried out in a way calculated to ensure the subject is unware it is taking place.

In determining whether a RIPA authority is required and may be authorised the case officer will need to consider and be able to explain to the authorising officer:

a) that the operation is in relation to a core investigatory activity

b) whether the offence which is under investigation is one which is punishable by a maximum term of at least 6 months imprisonment or is a specified offence relating to the sale of alcohol or is a specified offence relating to the sale of tobacco

c) that covert surveillance is necessary and proportionate to the matter under investigation

d) that there are no alternative means of obtaining the evidence

e) that a collateral intrusion risk assessment has been carried out

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, specific authorisation needs to be obtained. The case officer will need to complete the relevant parts of the authorisation form and one of the Council’s appropriately trained and authorised officers will need to consider the application and complete the authorising officers statement on the forms.

Applications for authorisations need to be framed in such a way that they do not require sanction from any person in the public authority other than the authorising officer (and magistrate).

Both 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, why and hows” of the authorisation. It must be clear who has been authorised to do what, when they can carry it out and how they are to undertake the surveillance. Necessity and proportionality cannot merely be inferred from the gravity of the offence, and clear reasoning must be provided. The codes of practice provide further guidance as to necessity and proportionality and these terms are explored further in officer training.

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

a) Is the surveillance for a relevant offence?

b) Is the surveillance necessary for the purpose of preventing or detecting crime? 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.

d) What are the implications arising from a collateral intrusion risk assessment?

In simple terms can the objective of the surveillance be important enough to justify the interference with an individual’s liberty and privacy and the risks of obtaining information about third parties?

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.

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.

There is specific guidance in the code of practice regarding surveillance that may yield confidential information which includes:

- 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 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 as it will be the authorising officer who needs to provide evidence to the magistrate as to why the authorisation is needed.

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 may reject 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 it may be possible to arrange this out of hours/outside of a court location.

Elected members, or members of council staff who are magistrates are obviously unable to authorise RIPA applications for council operations.

Particular circumstances

In all cases, this policy requires investigating officers to undertake early engagement with authorising officers to discuss potential RIPA implications of their investigations. A number of particular circumstances and techniques are discussed below.

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 must 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 digital media 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.

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 original intended use.

Online activities

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 human 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.

The latest code of practice provides more information regarding RIPA and online activities and training courses for council officers have been adjusted to take account of this. The general position is that whilst the internet is open to all, it should be viewed as no different to a public place, and as such there could be an expectation that a targeted operation to gather information from the internet regarding a specific person could fall within the scope of needing an authorisation. The application of surveillance laws to the internet is a developing field and as such it is helpful to provide pointers as to the matter of degree as to whether an authorisation is less or more likely to be required.

Use of the internet for an investigation (see para 3.10 – 3.17 of CoP)	
Factors making the need for an authorisation less likely	**Factors making the need for an authorisation more likely**
One off visit	Frequent visits to the same site
General search	Specific search for an individual
No recording of information	Information recorded for future use
No patterns of an individual's behaviour built up	Information provides a pattern of an individuals lifestyle

Tracking devices

Tracking devices which only provide position data do not fall within the scope of RIPA, however the installation of tracking devices onto third party property is likely to constitute property interference and as such an authorisation under the Police Act 1997 would be required. The council is not able to grant such authorisation.

Drones and unmanned Arial vehicles (UAV)

The council does not own UAVs, but from time to time may wish to make use of them. In general the use of a UAV to gather general data would not usually need an authorisation, however, if it is used as part of a specific operation to target an individual then authorisation would need to be considered. If a UAV is to be used for general purposes then whilst not needing a RIPA authorisation, permission from the relevant Portfolio Holder is required before the UAV is deployed.

Noise nuisance and similar recordings

This policy requires that recordings made to assist with determination of neighbour nuisance, ASB and similar must be done overtly. The code of practice discusses the application of RIPA to such circumstances and recognises that noise monitoring equipment which only records decibel levels would never need an authorisation. However, whilst covert techniques which record actual sound, and conversations at normal speaking level may well need consideration for authorisation, they are unlikely to pass the tests for an authorisation to be granted meaning they cannot be carried out covertly. Therefore the council's policy is that such recordings must be carried out overtly, and the council's corresponding noise policies reflect this. Additionally when officers ask members of the public to complete "diary/log sheets" or invite them to make their own audio or video recordings great care must be taken to avoid establishing a CHIS.

Authorising Officers

The Council currently have three trained officers who may authorise investigations. (Authorising Officers) These are:

- **Joanna Harding**
  Head of Public Health and Protection
  01707 357361
  jo.harding@welhat.gov.uk
- **Alison Marston**
  Governance Services Manager
  01707 357444
  a.marston@welhat.gov.uk
- **Kate Payne**
  Licensing Team Leader
  01707 357206
  k.payne@welhat.gov.uk

NOTE: 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 legislation and code of practice sets out the required level of authorisation for local authorities as the Head of Paid Service (the Chief Executive) or in their absence a Director acting as Head of Paid Service.

The Principal Governance Officer is the designated single point of contact (SPOC) for RIPA matters. This post is currently held by Jonah Anthony, j.anthony@welhat.gov.uk.

Undertaking surveillance

Once an authorisation has been granted by a magistrate 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.

Review and renewals

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.

Authorising Officers may renew applications to conduct surveillance 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.

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.

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 five 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.

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.

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.

As part of the annual “management assurance” process Heads of Service will be required to submit declarations with regard to the use of RIPA within their teams

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 five years from the ending of each authorisation.

At the Council this will be held by the Head of Law and Administration 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.

Mandatory reporting

The code of practice sets out new requirements with regard to error reporting and places duties on the Senior Responsible Officer to investigate and if necessary report errors in a particular way.

Examples of particular errors which would require investigation and reporting are that surveillance has taken places without lawful authorisation or there has been a failure by the council to adhere to the safeguards set out in the relevant statutory provisions and codes of practice. This policy commits the council to providing sufficient resources to enable the Senior Responsible Officer to investigate and report on any such errors. This error investigation and reporting mechanism is separate from the council complaints process and the right of an individual to complaint to the Commissioners or relevant Ombudsman.

Having submitted an error report, this policy commits the council to following any subsequent guidance issued by the Commissioner.

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.

Complaints

RIPA has established an independent Tribunal known as the Investigatory Powers Tribunal (IPT) made up of senior members of the judiciary and legal profession and is independent of the Government. This tribunal has jurisdiction to investigate and determine complaints against the use of surveillance powers by public authorities (including the council).

The code of practice states that any complaint about the use of surveillance powers should be referred to the IPT, although it is accepted that some complaints may come through the normal council complaint process. Therefore this policy requires any council officer in receipt of a complaint regarding surveillance powers to make the Senior Responsible Officer aware so that the complainant can be advised of their right to refer the matter to the IPT and also the need for any mandatory error investigation and reporting can be considered.

The IPT many be contacted at: Investigatory Powers Tribunal, PO Box 33220, London SW1H 0ZQ

https://www.ipt-uk.com

The IPT can advise on any rights of appeal against their decision.

Additionally dependent on the nature of the complaint the complainant may also wish to contact the Local Government and Social Care Ombudsman. https://www.lgo.org.uk/