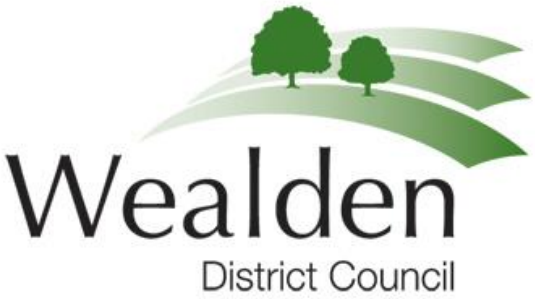

POLICY AND GUIDANCE ON THE REGULATION OF INVESTIGATORY POWERS ACT

2000

Introduction

1. The Regulation of Investigatory Powers Act 2000 ("RIPA") regulates the work of the council relating to surveillance, the use of covert human intelligence sources ("CHIS") and the accessing of certain communications data through a single point of contact (SPOC). It provides a legal framework for authorising investigations in a manner consistent with obligations under the Human Rights Act 2000 ("HRA") where the investigation is for the purposes of preventing or detecting crime. The Protection of Freedoms Act 2012 now means all applications for directed surveillance or CHIS have to have judicial approval.

   The Investigatory Powers Act 2016 has made some changes to the Regulation of Investigatory Powers Act 2000 which does impact on Local Authorities. It also replaces the role of the Surveillance Commisioners Office and the Interception of Communications Commissioners Office and merges them into one with wide ranging powers to inspect all public services.

   Local Authorities (LAs) **CANNOT** authorise directed surveillance, unless this involves a criminal offence(s) punishable (whether on summary conviction or indictment) by a maximum term of at least 6 months' imprisonment.

2. RIPA is wide ranging in its application and will impact all officers with an enforcement or investigatory capacity, including internal investigations. Failure to comply with RIPA may result in a claim for a breach of the Human Rights Act (HRA). This may result in evidence being deemed inadmissible in a prosecution or even a claim for compensation for an infringement of that person's human rights.

3. The Council is committed to implementing RIPA in a manner that is consistent with the spirit and letter of RIPA and the HRA. The Council is committed to conducting all relevant actions in a manner which strikes a balance between the rights of the individual and the legitimate interests of the public.

4. The Council's Chief Legal Officer (CLO) will act as the Senior Responsible Officer (SRO) under the Act and shall maintain a central record of all applications for authorisation.

Codes of Practice

5. Statutory Codes of Practice supplement RIPA. These deal respectively with covert surveillance, CHIS, interception of communications, communications data and electronic information. They are available on the following web link:

   http://security.homeoffice.gov.uk/ripa/counter-terrorism/regulation-investigatory-powers/ripa-codes-of-practice/

6. The Council's policy recognises the important role these Codes of Practice play in the practical implementation of RIPA. The Council will conduct all of its activities relating to RIPA whilst having due regard to and whilst following the recommended guidance contained within the Codes of Practice. It is essential, therefore, that all relevant officers involved in RIPA are familiar with the content of these Codes of Practice.

7. Any Officer who is uncertain or unsure about any aspect of this Policy, the Act or the Codes of Practice should contact the Council's Chief Legal Officer or the Council's Gate Keeper (GK) for advice and assistance.

8. On 1 November 2012 Protection of Freedoms Act provisions under the Regulation of Investigatory Powers Act 2000 (RIPA) changed the way in which LAs can apply and use Directed Surveillance (DS) and Communications Data (CD) and Covert Human Intelligence Sources (CHIS).

9. From 1 November 2012, sections 37 and 38 of the Protection of Freedoms Act 2012 came into force. This will mean that a LA who wishes to authorise the use of directed surveillance, acquisition of CD and use of a CHIS under RIPA will need to obtain an order approving the grant or renewal of an authorisation or notice from a District Judge or lay magistrate (JP) before it can take effect. If the JP is satisfied that the statutory tests have been met and that the use of the technique is necessary and proportionate he/she will issue an order approving the grant or renewal for the use of the technique as described in the application.

10. The new judicial approval mechanism was introduced in addition to the existing authorisation process under the relevant parts of RIPA as outlined in the Codes of Practice. The LA process of assessing necessity and proportionality, completing the RIPA authorisation/ application form and seeking approval from an authorising officer/ designated person will remains the same.

Surveillance

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

12. Similarly, surveillance will be overt if the subject has been told that it will happen.

Examples of Overt surveillance and <u>not</u> Directed Surveillance:

A. Activity that is observed as part of normal duties
B. CCTV cameras – unless they have been directed as the request of investigators, these are overt or incidental surveillance
C. Targeting a 'Jot Spot' e.g. licensing officers standing on a street to monitor private hire cars plying for hire illegally where this is not part of a planned operation, or standing on a street that has a high incidence of dog fouling
D. Test purchases for sale of alcohol to under 18s

13. Covert surveillance is defined in section 26(9)(a) of RIPA as any surveillance which is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place. It may be either direct or intrusive surveillance.

14. Directed surveillance is defined in section 26(2) of RIPA as surveillance which is covert, but not intrusive, and 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 RIPA to be sought for the carrying out of the surveillance.

15. The Code of Practice for Covert Surveillance and Property Interference provides detailed guidance on whether covert surveillance activity is directed surveillance or intrusive, or whether an authorisation for either activity would not be deemed necessary. That detailed guidance is not repeated here and officers are therefore directed to the Code of Practice for that information.

Examples of Directed Surveillance

Officers wish to drive past a café for the purposes of obtaining a photograph of the exterior. Reconnaissance of this nature is not likely to require a directed surveillance authorisation as not private information about any person is likely to be obtained or recorded. If the officers chanced to see illegal activities taking place, these could be recorded and acted upon as an 'immediate response to events'

If, however, the officers intended to carry out the exercise at a specific time of day, when they expected to see unlawful activity, this would not be reconnaissance but directed surveillance, and an authorisation should be considered.

Or if the officers wished to conduct a similar exercise several times, for example to establish a pattern of occupancy of the premises by any person, the accumulation of information is likely to result in the obtaining of private information about that person or persons and a directed surveillance authorisation should be considered.

16. Intrusive surveillance is defined in section 26(3) of RIPA as 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.

17. **Local Authorities are NOT authorised to conduct Intrusive Surveillance.**

18. The techniques which LAs may use

    a. **Directed surveillance** is essentially covert surveillance in places other than residential premises or private vehicles.
    b. LAs cannot conduct 'intrusive' surveillance (i.e. covert surveillance carried out in residential premises or private vehicles) under the RIPA framework.
    c. A **covert human intelligence source (CHIS) includes** undercover officers, public informants and people who make test purchases.
    d. **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). RIPA groups CD into three types:

19. A device used to enhance your external view of a property is almost never intrusive surveillance. A device would only become intrusive where it provided a high quality of information from inside the private residential premises.

Examples are:

A. Officers intend to use an empty office to carry out surveillance on a person who lives opposite. As the office is on the 4th floor they wish to use a long lens and binoculars so that they can correctly identify and then photograph their intended subject covertly. This is NOT intrusive surveillance as the devices do not provide high quality evidence from inside the subject's premises.

B. Officers intend using a surveillance van parked across the street from the subject's house. They could see and identify the subject without binoculars but have realised that, if they use a 500mm lens, as the subject has no net curtains or blinds, they should be able to see the document he is reading. This IS intrusive surveillance as the evidence is of a high quality, from inside the premises and is as good as could be provided by an officer or a device being on the premises.

20. A CHIS is defined in section 28(8) of RIPA as a person who:
    a. establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling with paragraph (b) or (c);
    b. he/she covertly uses such a relationship to obtain information or to provide access to any information to another person; or
    c. he/she covertly discloses information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship.

21. There is a separate revised code of practice for the use of human intelligence sources that again come into effect in April 2010. Again officers are directed to that code of practice for detailed guidance and examples.

Examples of CHIS may include: A. Licensing officers, working with the Police, covertly building a business relationship with a cab company which is believed to be using unlicensed drivers. B. Whistleblowing, when an employee is actively recruited to gather information on another employee who is the subject of a criminal investigation. C. Planning officers posing as customers to get information about the commercial activities at premises and developing a relationship with the workers beyond that of supplier and customer.

Communications Data (CD)

The new Investigatory Powers Act 2016 has created an offence under section 11 of unlawfully obtaining communications data from a communications or postal operator. This is where a "relevant person" holds an office, Rank or position with a relevant public authority. It carries a term of up to 12 months imprisonment and or a fine upon conviction. This section includes ANY communications provider and ANY postal provider.
Under section 3 of the Act it is an offence to intercept ANY communications in the course of its transmission this also includes Postal services.
A postal operator for both sections includes courier companies and services.

22. For CD requests, a Single Point of Contact (SPOC) undertakes the practical facilitation with the communications service provider (CSP) in order to obtain the CD requested. They will have received training specifically to facilitate lawful acquisition of CD and effective co-operation between the local authority and communications service providers.

    The SPOC for all RIPA applications is with the National Anti-Fraud Network (NAFN) who can be contacted via the LA GK.

23 LAs unable to call upon the services of an accredited SPOC should not undertake the acquisition of CD.

24 For CD requests the Home Office envisages that the local authority may also choose to authorise, under section 223 of the Local Government Act, their GK in order that they may appear in front of the JP. In cases where the type of CD or its retrieval is technically complex and the JP wants to satisfy him/herself that the CD sought meets the test, then the SPOC may be best placed to explain the technical aspects.

25. Following the hearing the SPOC may acquire the data. SPOC must not acquire the data via a CSP or using automated systems until after the JP has signed the order approving the grant. The one month time limit will commence from the date of the JPs signature giving approval.

26. The National Anti-Fraud Network provides a SPOC service to local authorities, precluding each authority from the requirement to maintain their own trained staff and allowing NAFN to act as a source of expertise. LAs using the NAFN SPOC service will still be responsible for submitting any applications to the JP and a designated person in the local authority is still required to scrutinise and approve any applications. The accredited SPOCs at NAFN will examine the applications independently and provide advice to applicants and designated persons to ensure the local authority acts in an informed and lawful manner.

27. The LA investigator (i.e. the applicant) will then submit the relevant judicial application/order form, the RIPA application (authorisation or notice) and any supporting material to the JP. As above, following a private hearing, the JP will complete the order section of the judicial application/order form, reflecting their decision. The local authority investigator will then upload a copy of this order to the NAFN SPOC.

28. The NAFN SPOC will then acquire the CD on behalf of the local authority in an efficient and effective manner.

29. In addition to carrying out covert surveillance and the use of a CHIS, the Council may also access certain communications data under RIPA, provided this, like all other surveillance, is **for the purpose of preventing or detecting crime only.**

30. All applications for telecom data also require judicial approval. (The codes of practice shall be followed at all times. Council staff are not permitted to obtain telecommunications and internet use data other than as provided for by the Act.)

31. Authorisations and notices for CD will be valid for a maximum of one month from the date the JP has approved the grant. This means that the conduct authorised should have been commenced or the notice served within that month.

32. Communications data as defined by Section 21(4) of the Act. **However, the Council may only acquire communications data falling within sections 21(4)b and 21(4)c of the Act.** In essence the Council may acquire certain information held by communication service providers relating to their customers. However, communications data does **NOT** include the content of any communication.

Authorising Officer

33. All requests for authorisation of directed surveillance or a CHIS under RIPA must be approved in advance by an Authorising Officer. An Authorising Officer is a person who has been delegated power to act in that capacity by the CLO or relevant Corporate Director with regulatory responsibilities. A list of officers who have, to date, been authorised, is annexed to this policy and is subject to regular review and updating by the CLO.

34. In order to be approved as an Authorising Officer, that person must have attended a relevant training course on the practical application of RIPA.

G**ate Keeper** (GK)

35. The Council operates a GK system for all authorisations. Prior to submitting an application for directed surveillance or a CHIS to an Authorising Officer, you MUST first submit the forms to the GK. Details of who is authorised to act as GK are set out in the Appendix to this policy.

36. The GK will act as a form of quality control and will advise the applicant on any aspect of your proposed surveillance operation, including the way in which they must complete their application for directed surveillance or CHIS.

Authorisation Process

37. All requests to conduct, renew, review or cancel a covert surveillance exercise or use of a CHIS must be made in advance in writing on the appropriate forms. Following advice from the GK, all such requests must be submitted to an Authorising Officer of the Council. To ensure the latest forms are used, please download the relevant version from the Home Office website, via the following link:

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

38. The Local Authority will have an Authorising Officer with the power to renew, review and cancel directed covert surveillance in order to ensure greater independence and consistency. Only after the Authorising Officer has provided written authorisation for a directed covert surveillance can the application be presented to a Justice of the Peace.

39. The current time limits for an authorisation or notice will continue. That is: 3 months for directed surveillance and 12 months for a CHIS (1 month if the CHIS is 18 years old or under). Authorisations and notices for CD will be valid for a maximum of one month from the date the JP has approved the grant. This means that the conduct authorised should have been commenced or the notice served within that month.

40. A renewal must be authorised prior to the expiry of the original authorisation, but it runs from the expiry date and time of that original authorisation. Authorisations may be renewed more than once if still considered necessary and proportionate and approved by the JP.

41. Prior to submitting the forms, the applicant must obtain a unique reference number for their application. This is generated through the central record of authorisations. The applicant should contact the CLO to obtain the next unique number.

42. When completing the forms, a full and detailed description of the operation should be provided. This should specify any equipment to be used as well as maps or sketches to show observation points and target premises. Officers need to take particular care to ensure there are no ambiguities in the description of the operation.

43. RIPA first requires that the Authorising Officer and the Justice of the Peace before granting an authorisation, believe that the authorisation is necessary in the circumstances of the particular case for the statutory basis grounds for directed surveillance or a CHIS; namely that the proposed activity is necessary for the prevention and detection of crime or prevention disorder. This is the **ONLY** ground that a local authority can apply for and be granted authorisation under the act.

44. The application should identify:

    (a) the specific offence being investigated
    (b) the specific point to prove that the surveillance is intended to gather evidence about
    (c) that the operation is capable of gathering that evidence; and
    (d) that such evidence is likely to prove that part of the offence.
    (e) how any third party information might be obtained and how that would be dealt with.

45. Then, if the directed surveillance or use of the CHIS is necessary, the person granting the authorisation must believe that the directed surveillance or use of a CHIS is proportionate to what is sought to be achieved by the conduct and/or use of that CHIS. This involves balancing the intrusiveness of the surveillance or use of the CHIS on the target and others who might be affected by it against the need for the surveillance or CHIS to be used in operational terms. The use of surveillance or a CHIS will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by

other less intrusive means. The use of surveillance or a CHIS should be carefully managed to meet the objective in question and sources must not be used in an arbitrary or unfair way.

46. Proportionality must be carefully explained, not merely assented. Similarly, merely describing parts of the operation itself is not germane to proportionality. A good explanation of proportionality should refer to three elements:

    (a) balance the extent of the problem against the size and scope of the operation, demonstrating that it is not a 'sledgehammer to crack a nut',
    (b) explain that intrusion is to be kept to a minimum
    (c) show that having considered all other practical courses there is no other way in which the necessary evidence can be obtained i.e. a cover operation is the last resort.

47. The Authorising Officer must state their reasons for believing that the authorisation, renewal or cancellation is necessary. If they do not consider authorisation, renewal or cancellation to be appropriate they must also state their reasons for this on the relevant form.

48. The Authorising Officer's statement should not be a mere rubberstamp. It should include a full account of what is being authorised (the five W's test of Who, What, Why, Where & When) and how and why the Authorising Officer is satisfied that the operation is necessary and proportionate. A bare assertion is insufficient.

49. The application MUST make it clear how the proposed intrusion is necessary and how an absence of this evidence would have a prejudicial effect on the outcome of the investigation.

50. The Authorising Officer should not be put off by repetition as if challenged in court, the Authorising Officer may be required to demonstrate his own thought process at the time and will be in a weak position if he has to rely upon the applicant's account by adoption.

51 A Justice of the Peace when granting such an Authorisation must also state their reason for granting this, in writing, on the application form. The Justice of the Peace must also provide written explanation should they reject or defer an authorisation.

Collateral Intrusion

52. Before authorising the use or conduct of a source, the authorising officer should also take into account the risk of intrusion into the privacy of persons other than those who are directly the subjects of the operation or investigation (collateral intrusion). Measures should be taken, wherever practicable, to avoid unnecessary intrusion into the lives of those not directly connected with the operation.

53. An application for an authorisation should include an assessment of the risk of any collateral intrusion. The authorising officer should take this into account when considering the proportionality of the use and conduct of a source.

Practical Considerations

54. The Council's requirements for covert surveillance will normally be carefully planned so that the necessary consultations regarding risk assessment, insurance and health and safety can be carried out and the required provisions put in place before surveillance commences.

55. In the event of covert surveillance needing to be carried out in an emergency, authorisation is still required. Where it is not possible for the requesting officer to complete the form, the Authorising Officer must still be consulted. A Local Authority is NOT able to carry out any surveillance without written authorisation, however an officer should consider whether the offence being investigated would carry a minimum sentence of more than six months imprisonment and the level of required authorisation needed.

56. General observation forms part of the duties of many enforcement officers and is not usually regulated by RIPA. For example, Community Wardens may be on patrol to observe or prevent crime. Such observation may involve the use of equipment to merely reinforce normal sensory perception, such as binoculars, or the use of cameras, where this does not involve systematic surveillance of an individual.

57. Directed surveillance does not include covert surveillance carried out by way of an immediate response to events or circumstances which, by its very nature, could not have been foreseen. For example, a community warden would not require an authorisation to conceal him or herself and observe a suspicious person that s/he came across in the course of a patrol. If later, however, a specific investigation or operation is to follow an unforeseen response, authorisation must be obtained in the usual way before it can commence. In no circumstance will any covert surveillance/ use of a CHIS be given backdated authorisation after it has commenced.

58. Embarking upon covert surveillance or the use of a CHIS without authorisation or conducting surveillance outside the scope of the authorisation will not only mean that the protection afforded by RIPA is negated but may also result in disciplinary action being taken against the Officer/Officers involved.

59. Although, the provisions of RIPA do not normally cover the use of overt CCTV surveillance systems, since members of the public are aware that such systems are in use, there may be occasions when public authorities use overt CCTV systems for the purposes of a specific investigation or operation. In such cases, authorisation for directed surveillance will be necessary.

60. Material obtained through covert surveillance may be used as evidence in criminal proceedings. The proper authorisation of surveillance should ensure the admissibility of such evidence under the common law, section 78 of the Police and Criminal Evidence Act 1984 and the Human Rights Act 1998. Furthermore, the product of the surveillance described in this code is subject to the ordinary rules for retention and disclosure of material under the Criminal Procedure and Investigations Act 1996.

61. Whilst acknowledging that covert surveillance/use of a CHIS is a last resort, RIPA does afford potential protection against claims of unlawful action. Officers must seek the view of an Authorising Officer if they are in any doubt as to whether RIPA is likely to apply to their investigation or action.

62. Where the use of a CHIS is deployed, a “Handler”, who can be an officer of the Council, should be designated to have day to day responsibility for dealing with the CHIS. This will include their security, safety and welfare.

63. The only circumstances where authorisation may be given under this regime is where the investigation is for the purpose of preventing or detecting crime or for preventing disorder.

Special Circumstances

64. The use of vulnerable people/juveniles for a CHIS should only occur in exceptional circumstances and due regard must be had to the Code of Practice.

65. Likewise, if covert surveillance is likely to obtain communications subject to legal privilege, or involve confidential personal or journalistic information or material, the officer should refer to the Code of Practice. An authorisation will then only be merited in exceptional or compelling circumstances.

66. Where Special Circumstances apply officers must obtain authorisation for the action from either the Chief Executive, the relevant Corporate Director of Service, the CLO or the Head of Business Services.

Social Media

67. Public authorities now make use of the wide availability of details about individuals, groups or locations that are provided on social networking sites, or open source on the internet. This information **IS NOT** fair game and any repetitive access of an individual’s social network sites for the purpose of intelligence gathering or data collection will require authorisation under RIPA.

68. The (SRO) should ensure that all staff within the LA are fully aware of the restrictions that govern accessing social media sites. Any such access to these sites should be undertaken with a suitable authorisation to ensure

that the right to privacy and matters of collateral intrusion have been adequately considered and staff have not been placed at risk by their actions or have not placed the council at risk by breaching the HRA.

69. Officers using social media as part of an investigation will have to ensure that they are fully aware of the restrictions and at what point they would require either a directed surveillance authorisation or even the need for CHIS authority. Any such circumstances would need to be discussed with the GK and the SRO before they go ahead.

    Repetitive and systematic access would be viewing such sites on more than one occasion in order to view activity and obtain personal data of the individual's site.

Partnership Working

70. If conducting a relevant RIPA investigation in partnership with, under the direct guidance or supervision of, or under a request from another body, officers must first seek the approval of an Authorising Officer.

71. When another agency wishes to use the Council's resources that agency must use its own RIPA procedures. Before any Officer agrees to permit the use of Council resources, they must obtain a copy of that agency's RIPA form for the record, and/or relevant extracts from the form.

Equipment

72**.** The council will keep a spreadsheet of all equipment used for surveillance or with a particular authorisation. There are certain specialist pieces of equipment that have their own operating instructions and controls. The council's planning department own 2 radio controlled drones which carry cameras or thermal imaging cameras. The drones are used for planning purposes and overtly by trained and authorised operators, there are strict operating instructions and the use of the drones in a covert situation have been considered and guidance issued. (Appendix A, Annex 2).

73. The council also has a standalone IPad which is used for open source research. This is used mainly by staff wishing to trace customers who owe a substantial debt to the council or who are being investigated for offences of Fraud. There are also separate and strict guidance on the use of this IPad, most enquiries are made on a one off basis and fall outside of the regulations. Any repetitive use or viewing will require a directed surveillance authorisation and will be subject to short reviews by the authorising officer.

Training

74. All officers with an enforcement or investigatory function will receive training on the provisions of RIPA. Minimum requirement for such officers will be to receive such training on an annual basis.
75. The responsibility of the GK is not only to ensure that he/she is up to date on all RIPA and Property Interference legislation, but also to be fully briefed on all current policies issued from the Investigatory Powers Commissioners Office (IPCO).

    The GK will be responsible for delivering a training programme for all staff relating to the use of social media sites within the work place. The use of social media sites by staff is considered to be a high risk area for the council and training is essential in order to enhance staff awareness about using such sites.

Central Record of all authorisations

76. The GK will maintain a register of all applications and authorisations obtained on behalf of the Local Authority.

77. Each Authorising Officer will be responsible for maintaining a record of all authorisations, renewals, reviews and cancellations issued by them.

78. The Authorising Officer will also be responsible for forwarding a copy of each and every form completed for that purpose to the Chief Legal Officer within one week of completing that form. The form should be sent in an envelope marked Private and Confidential and for the attention only of the CLO. The CLO will then maintain a Central Record of Authorisations.

79. These records will be retained for a period of at least three years from the ending of the authorisation and should contain the following information:
    - the type of authorisation;
    - the date the authorisation was given;
    - name and rank/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.
    - if the authorisation is renewed, when it was renewed and who authorised the renewal, including the name and rank/grade of the authorising officer;
    - whether the investigation or operation is likely to result in obtaining confidential information as defined in this code of practice;
    - the date the authorisation was cancelled.

80. The Audit & Investigations Manager will be responsible for monitoring authorisations and carrying out annual and random reviews of applications, authorisations, reviews, renewals and cancellations.

Authorisations outside of RIPA

81 There will be occasions in a LA investigations into offences where there is a need for some surveillance but the criteria for an authorisation under RIPA is not met, such as a non-criminal offence or the matter under investigation does not attract a minimum of 6 months in prison. Such matters can by authorised by the AO without the need of authorisation by a JP.

82. In such cases it will be the responsibility of the Investigating Officer (IO) to complete an application for RIPA authorisation and submit it via the GK to the LA's AO. The same processes must be followed by both the IO and AO in relation to necessity and proportionality. All time limits must also be adhered to and it will be the responsibility of the AO to ensure that such action is justified.
83. Authorisations granted in such circumstances would be very rare but may be used in circumstances where there is a necessity to access social media sites.

84. The most common occasion where an authorisation outside of the guidelines will be authorised is when an officer is using open source or social media sites as part of an ongoing investigation. There is a separate procedure in place in such circumstances and all such situations are subject to regular review by the GK or SRO.

Conclusion

85. The relevant portfolio holder will review this policy annually with the support and assistance of the CLO, Head of Business Services, and such other officers as the portfolio holder may require. In addition, the CLO will provide a quarterly report to the relevant portfolio holder on the use of the powers under the Act to ensure that the powers are being used consistently with the local authority's policy and that the policy remains fit for purpose.

86. All enquiries about this policy or the applicability of RIPA should be referred at first instance to the Head of Business Servicers or such other person as they may designate.

87. For additional information/guidance please see the Home Office or Office of the Surveillance Commissioners websites.

Annex 1

Current List of Authorising Officers

Charlie Lant
Nigel Hannam
Isobel Garden
David Palmer
Trevor Scott
Steve Linnett

Single Point of Contact

David Palmer

Gate Keeper

John Stalley

Annex 2

Guidance Notes

Authorisation will be required for a proposed activity if the answer is 'Yes' to all of questions 1-7 below:

If the answer is 'No' to any of them, the proposed activity will not be entitled to protection under RIPA and authorisation will not be granted so should not be the subject of an application request.

1. Is there a need for covert surveillance? Is it necessary and proportionate in accordance with the Act and the Code of Practice? The activity will not be proportionate if it is excessive in the circumstances or if the information could reasonably be obtained by other less intrusive means.
2. Is the proposed activity 'surveillance'? Will it comprise monitoring, observing or listening to persons, their movements, their conversations or their activities and/or recording anything monitored, observed or listened to in the course of the proposed activity?
3. Is it covert? Will the activity be carried out in a manner calculated to ensure that the target will be unaware that it is or may be taking place.
4. Is it directed? Will the activity be for the purpose of a specific operation or investigation?
5, Is it likely to result in the obtaining of private information about this person?
6. Is there a risk of obtaining private information about another person? (this is known as collateral intrusion). If so, has the necessary risk assessment been carried out and is the covert surveillance proportionate in the circumstances.
7. Is it a foreseen/planned response? Is it something other than an immediate response in circumstances where it is not reasonable to get an authorisation?

Other important matters:

a. Has a risk assessment been completed that identifies all relevant risks to staff in the conduct of the operation? This is particularly important where a CHIS is being deployed.
b. On completion of the authorisation, has the AO set a review date for reconsideration of the authorisation?
c. On completion of the surveillance, the Applicant must complete the cancellation form.
d. Ensure that the most up to date forms are used by downloading copies from the Home Office website on the link provided in the policy.

Annex 3

Wealden District Council
Use of Drones

To be read and used in conjunction with the Wealden District Council
Unmanned Aerial Vehicles Policy

1. Wealden District Council Planning Department have purchased two Drones to take pictures of sites, potential sites, buildings and developments and to assist with their activities and business.

2. A Drone is a small radio controlled aircraft that can carry small photographic/ video/ Thermol Imaging equipment.

3. The use of such an aircraft is strictly controlled by the regulations set out by the Civil Aviation Authority (CAA).

4. There is no doubt that some of the usage of the Drone will be classified as surveillance. The issue will be whether the usage is covert or overt surveillance and the necessary authorities would need to be in place for such activity.

5. Any surveillance by a public authority is governed by strict legislation; this is in the form of the Regulation of Investigatory Powers Act 2000 known as RIPA which ensures compliance with the ECHR 2000. Local Authorities are further governed by new legislation with the Protection of Freedoms Act 2012.

6. All Surveillance is further over seen by the Office of the Surveillance Commissioner (OSC) who publishes a guidance document which should be followed by Local Authorities (LA) who conduct surveillance operations. They make inspections of records kept by LA's every 3 years.

7. RIPA describes surveillance as being any surveillance which is carried out in a manner calculated to ensure that the persons subject to that surveillance are unaware that it is or may be taking place, as in Section 26 (9)(A) of the RIPA 2000.

8. The use of the Drones will mostly be overt and not covert. Drone operators will be wearing high visibility jackets that are clearly labelled or even uniform that is clearly labelled to show that they are from Wealden District Council and that they are Drone operators.

9. There will be signage placed in the area of the operations that will clearly show that there is a Drone being used and that operators will be using vehicles that are clearly marked and labelled as being from Wealden Council and the usage of drones is taking place.

10. This can be further enhanced by advising all applicants for planning permission that we operate Drones and that we use them for the purposes of viewing developments, sites and for possible breaches of planning rules and regulations.

11. There will be occasions when the Drone will be used for covert surveillance, but there are very strict rules and regulations governing its use. This type of surveillance would be called directed surveillance and is defined by the RIPA as being surveillance which is covert but not intrusive and is undertaken

    A. for the purpose of a specific investigation or specific operation

    B. in such a manner as likely to result in obtaining of private information about a person or persons whether or not one specifically identified for the purpose of the investigation or the operation and otherwise.

    C. By way of an immediate response to an event or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under Part 2 of RIPA to be sought for the carrying out of surveillance.

12. In such circumstances, the rules have recently changed as part of the Protection of Freedoms Act 2012. That piece of legislation states that all Local Authorities engaging in any form of directed surveillance **must** have the surveillance authorised through a Justice of the Peace.

13. The procedure starts with an application form from the person or the team wishing to conduct surveillance. This is then passed to the Gatekeeper for the Council. For Wealden District Council this is John Stalley in the Audit and Investigations Team.

14. The applicant will have shown that he has considered Article 8 of the Human European Convention on Human Rights (ECHR 2000), Right to a Private Life. They would also have to show that they have considered the justification, necessity and proportionality of the application. If the Gatekeeper is satisfied; that this criteria has been met, and that the offence for which the surveillance is needed attracts a minimum prison sentence of 6 months or more then he will forward the application to a Single Point of Contact (SPoC) at the National Anti-Fraud Network (NAFN) as this is the Government organisation that monitors all surveillance conducted by Local Authorities.

15. NAFN will forward the application back to one of the Local Authorities authorising officers. This will be a Director or a Senior Head of Service. For Wealden District Council the Authorising Officers are:

    Charlie Lant
    Nigel Hannam
    Isabel Garden
    Trevor Scott
    David Palmer
    Steve Linnett

16. The Authorising Officer will sign the application to say that they approve the surveillance on behalf of the Council. The form is then returned via NAFN to the Gatekeeper. The Gatekeeper will then arrange final authorisation with the local Magistrate. This process has to be completed before any surveillance can take place.

17. The authorisation will last for a period of 3 months, after which it has to be either cancelled or renewed prior to its expiry. The Authorising Officer for the Council may require a review at any time or at regular intervals during the 3 month period.

18. Once the objective for the surveillance has been achieved, the authorisation has to be cancelled immediately, with the completion of a cancellation form which has to be signed by the Authorising Officer and sent to NAFN. It has to clearly define what was achieved, what evidence was obtained and whether there was any collateral intrusion.

19. Collateral intrusion or third party information that is obtained but is not necessary has to be immediately disregarded and removed from the investigation. Private information is very strictly controlled and is known as collateral intrusion or third party information. Any such information that is obtained during the surveillance could be construed as being intrusive. Legislation strictly forbids any Local Authority from conducting intrusive surveillance.

20. Any such breaches would have to be reported to the Office of Surveillance Commissioner and the authority that had been granted would have to be reviewed and reconsidered.

21. The whole process is monitored by the Gatekeeper on behalf of the Council and the Authorising Officer. Copies of all applications renewals and cancellations have to be kept for inspection by the OSC.

Conclusion

The Drone can be used by Wealden District Council to provide photographic views of sites or proposed sites for planning and development. No authorisation is needed in the circumstances providing it is clearly shown that the Drone is being used overtly. If it is used for the prevention or detection of offences or breaches of regulations and is being used overtly, the use in such circumstances would need to be registered only within the Council.

In circumstance where the Drone would be used covertly for the prevention and detection of offences that attract 6 months imprisonment or more, then authorisation under RIPA has to be obtained before that surveillance can take place

Annex 4 – Legislation References

- Sec 30 – 32 Regulation of Investigatory Powers Act 2000.
- The Protection of Freedoms Act 2012
- ECHR 2000
- Under Planning and Enforcement we can also include: The Town and Country Planning (General Permitted Development) Order 2015, (as amended) and the Town and Country Planning (Use Classes) Order 1987 (as amended)
- **Planning enforcement:** Town and Country Planning Act 1990 (as amended), the Planning and Compensation Act 1991, (as amended), Control of Advertisements Act 2007 (as amended), **Planning (Listed Buildings and Conservation Areas) Act 1990, (as amended),** Caravan Sites and Control of Development Act 1960, (as amended), Caravan sites Act 1968, (as amended) and Human Rights Act 1998, (as amended)
- **Development management:** Town and Country Planning Act 1990 (as amended), the Planning and Compensation Act 1991, (as amended), Control of Advertisements Act 2007 (as amended), **Planning (Listed Buildings and Conservation Areas) Act 1990, (as amended),** Caravan Sites and Control of Development Act 1960, (as amended), Caravan sites Act 1968, (as amended) and Human Rights Act 1998, (as amended)
- **Building control:** The Building Act 1984, as amended

IPod Internet Access.

INTENTION:

- The purpose of having internet access via the IPod is to enable officers to use open web research facilities or Open Source Research. The internet is vast and most domestic users and organisations only access about 5% of it. The remaining 95% is known as the "Dark Web" but it contains vast amounts of untapped information that is of use to investigators.

- The "*dark web"* is used for research and intelligence gathering by Police, HMRC, UKBF, Military, Immigration, Security Services, Journalists, Debt collection agencies. The list is endless but the one thing that all these agencies have in common is that they are all investigators.

- Some of this research in the *"dark web"* can be regarded as contentious and may need to be covert if certain sites are visited on a regular basis to try and identify lifestyle patterns. Information on the internet is regarded as being in the public domain, however regular research on some social media site may infringe upon an individual's human rights (Article 8) and will need to be covered by the appropriate legislation, (Directed Surveillance under RIPA 2000)

- The IPad will be used to give an Internet Protocol Address (IPA) which is independent from any connected to Wealden District Council (WDC). The purpose of this is to provide anonymity for the user and device when being used for covert purposes and to provide protection to WDC in case the device is "hacked or intercepted or compromised" in any way. Also to protect the organisations IT systems from potential contamination from the various bugs, viruses and Trojans that are out on the internet at the moment.

Implementation:

- The Counter Fraud Team has an IPad which is used for internet access and note taking when the team are away from the office. IT have taken the IPad to give it a new identity that is not linked to WDC and will enable it to be used outside of the organisation where appropriate. A new and independent ISP has been opened solely for use with the IPad.

- The Wealden Counter Fraud Team and some of the Council Tax Enforcement Team have completed a one day course on the use of Open Source and *"dark web"* Evidence/Intelligence gathering. This was followed up with another one day course of RIPA 2000 training in relation to the use of internet searching in May 2016.

- The IPad will only be used by Officers who have completed the Open Source training. They will have to complete an access form log to demonstrate that the necessity, justification and proportionality have all been carefully considered to ensure compliance with the ECHR and the HR Act 1998 and RIPA 2000 and agreed with the RIPA Gatekeeper.

Management:

- The IPad will be kept in a locked cabinet used by the Counter Fraud Team. Any officer wishing to use it will have to book it out and back in again after they have finished using it.

- It cannot be taken home or used for personal use and can only be used for Open Searching in the Wealden Offices.

- A record of each search will be made on a form that will be kept by the Counter Fraud Team in case it is needed for scrutiny at a later date. They will be kept for a maximum of 3 years which is the visiting cycle of inspectors from the Office of Surveillance Commissioners (OSC).

- Most enquiries made on the IPad will be outside of the requirements of RIPA 2000. However this procedure formulated around a directed surveillance authorisation will be adhered to when using the IPad for research on the dark net. Proportionality, Lawfulness Accountability and Necessity (PLAN) will be complied with each time the device is used by one of the trained personnel, its use will be recorded and may be subjected to scrutiny by the RIPA Gatekeeper, or the DPA Officer for the Council.

Accountability:

- A log sheet will be completed each time the device is used (Appendix A) It will give the Officers name the time, day and date. The purpose of the search and the sites visited and any product found. It will then be filed and returned with the IPad to the Counter Fraud Team who will check the form and the PLAN before signing it back in.

- Each officer using the device will be held responsible for the sites they are visiting and the use of the IPad. If visits to a particular site is deemed necessary on a regular basis then an authorisation for Directed Surveillance will have to be applied for (Annex 3). If the offence under investigations does not attract a fine of over £1000 and/or a minimum of 6 months imprisonment then it will fall outside of the requirements of RIPA 2000.

- In such Case as defined above an authorisation WILL be obtained and signed off by one of the authorising signatories for Wealden Council. It will comply with the requirements of RIPA 2000 as far as PLAN is concerned and the terms of operation will be defined by the authorising

officer. The process of RIPA reviews, renewals and cancellations will be adhered to. Any such authorisations will be scrutinised by the councils “Gatekeeper” and kept for scrutiny by the OSC.

Conclusion:

- The usage of the IPad will be strictly controlled and recorded
- It will be managed through the Counter Fraud Team and the Council’s RIPA gatekeeper.
- All searches will be subject to scrutiny and compliant with the Human Rights Act 1998 Articles 6 & 8.
- The device can only be used at Wealden Council Offices and will be kept locked and secure when not being used.
- Only officers who have completed an open source and RIPA 2000 courses will be able to use the device.

****

Recording Open Source Enquiries

Operators name:		Desired outcome	
Date & Time	Site	Search Terms (if applicable)	Product (including print reference)

Part II of the Regulation of Investigatory Powers Act 2000

Authorisation Directed Surveillance

Public Authority *(including full address)*			
Name of Applicant		**Unit/Branch/Division**	
Full Address			
Contact Details			
Investigation/Operation Name (if applicable)			
Investigating Officer (if a person other than the applicant)			

DETAILS OF APPLICATION

1. Give rank or position of authorising officer in accordance with the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 No. 521. [1]

2. Describe the purpose of the specific operation or investigation.

3. Describe in detail the surveillance operation to be authorised and expected duration, including any premises, vehicles or equipment (e.g. camera, binoculars, recorder) that may be used.

4. The identities, where known, of those to be subject of the directed surveillance.

- Name:
- Address:
- DOB:
- Other information as appropriate:

5. Explain the information that it is desired to obtain as a result of the directed surveillance.

[1] For local authorities: The exact position of the authorising officer should be given. For example, Head of Trading Standards.

6. Identify on which grounds the directed surveillance is <u>necessary</u> under Section 28(3) of RIPA. *Delete those that are inapplicable. Ensure that you know which of these grounds you are entitled to rely on (SI 2010 No.521).*

- In the interests of national security;
- For the purpose of preventing or detecting crime or of preventing disorder;
- In the interests of the economic well-being of the United Kingdom;
- In the interests of public safety;
- for the purpose of protecting public health;
- for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;

7. Explain <u>why</u> this directed surveillance is necessary on the grounds you have identified [Code paragraph 3.3].

8. Supply details of any potential collateral intrusion and why the intrusion is unavoidable. [Bear in mind Code paragraphs 3.8 to 3.11.]

Describe precautions you will take to minimise collateral intrusion.

9. Explain <u>why</u> this directed surveillance is proportionate to what it seeks to achieve. How intrusive might it be on the subject of surveillance or on others? And why is this intrusion outweighed by the need for surveillance in operational terms or can the evidence be obtained by any other means [Code paragraphs 3.4 to 3.7]?
10. Confidential information [Code paragraphs 4.1 to 4.31]. INDICATE THE LIKELIHOOD OF ACQUIRING ANY CONFIDENTIAL INFORMATION:

11. Applicant's Details

Name (print)		**Tel No:**	
Grade/Rank		**Date**	
Signature			

12. Authorising Officer's Statement. [Spell out the "5 Ws" – Who; What; Where; When; Why and HOW– in this and the following box.]

I hereby authorise directed surveillance defined as follows: [*Why is the surveillance necessary, whom is the surveillance directed against, Where and When will it take place, What surveillance activity/equipment is sanctioned, How is it to be achieved?]*

13. Explain <u>why</u> you believe the directed surveillance is necessary [Code paragraph 3.3]. **Explain <u>why</u> you believe the directed surveillance to be proportionate to what is sought to be achieved by carrying it out [Code paragraphs 3.4 to 3.7].**
14. (Confidential Information Authorisation.) Supply detail demonstrating compliance with Code paragraphs 4.1 to 4.31.

Date of first review	

Programme for subsequent reviews of this authorisation: [Code paragraph 3.23]. Only complete this box if review dates after first review are known. If not or inappropriate to set additional review dates then leave blank.

Name (Print)		**Grade Rank**	
Signature		**Date and time**	
Expiry date and time [e.g.: authorisation granted on 1 April 2005 - expires on 30 June 2005, 23.59]			

15. Urgent Authorisation [Code paragraph 5.9]: Authorising officer: explain why you considered the case so urgent that an oral instead of a written authorisation was given.
16. If you are only entitled to act in urgent cases: explain why it was not reasonably practicable for the application to be considered by a fully qualified authorising officer.

Name (Print)		**Grade/Rank**		
Signature		**Date and Time**		

Urgent authorisation Expiry date:		**Expiry time:**	
Remember the 72 hour rule for urgent authorities – check Code of Practice.	e.g. authorisation granted at 5pm on June 1st expires 4.59pm on 4th June		