Walsall Council

Regulation of Investigatory Powers Act 2000

Surveillance and Covert Human Intelligence Source Policy and Procedure

Page left intentionally blank

Contents

	Glossary & Relevant Links
1 1.	Policy Statement
2	Legislative background
3	Surveillance
3.2	Overt Surveillance
3.3	Covert Surveillance
3.6	Covert Directed Surveillance
3.7	Directed Surveillance Crime Threshold
3.9	Covert Intrusive Surveillance
3.13	Non RIPA Authorisations
4	Private Information
5	Confidential Information
6	Covert Human Intelligence Source CHIS
7	Vulnerable Individuals/Juvenile CHIS
8	CCTV
9	Use of Social Media/Internet
10	Aerial Surveillance
11	Residential Premises & Private Vehicles
12	Restrictions on Certain Activities
13	Authorisation Procedures
13.1	Authorising Officers for Directed Surveillance and CHIS
13.7	Authorisation of Covert Directed Surveillance and Use of a CHIS
14	The Magistrates Court
15	The procedure for applying for directed surveillance or use of a CHIS
16	Additional Requirements for Authorisation of a CHIS
17	Urgent Authorisations
18	Review of Authorisations
19	Renewal of Authorisations
20	Cancellation of Authorisations
21	What Happens if Surveillance has Unexpected Results
22	Errors
23	Records of RIPA Authorisation
24	Handling of Material and Safeguards
25	Use of Material as Evidence
26	Disseminating Material
27	Copying Material
28	Storage of Material
29	Retention and Destruction of Material
30	Surveillance Products
31	Training and advice and departmental policies, procedures and codes of conduct.
32	Complaints
APPENDIX 1 Non RIPA Authorisations APPENDIX 2 List of Authorised Officer Posts for Authorising Directed surveillance APPENDIX 3 Legilation	

Glossary

ANPR	Automated Number Plate Recognition
AO	Authorising Officer
CCTV	Closed Circuit Television.
CHIS	Covert Human Intelligence Source.
DVLA	Driver and Vehicle Licensing Agency
ECHR	European Contention on Human Rights
HRA	Human Rights Act 1998.
JP	Justice of the Peace
IPCO	Investigatory Powers Commissioners Office
RIPA	Regulation of Investigatory Powers Act 2000
SNS	Social Network Sites
SRO	Senior Responsible Officer.

Relevant Links

The Home Office have provided information relating to RIPA on the GOV.UK website

https://www.gov.uk/government/collections/ripa-codes

Forms relating to the use of RIPA can also be found at GOV.UK

https://www.gov.uk/government/collections/ripa-forms--2

If blank documents are stored locally regular checks ought to be made to ensure the forms remain up to date with current legal or best practice changes.

1. Policy Statement

1.1 The objective of this policy and procedure is to ensure that all investigations within the scope of the Regulation of Investigatory Powers Act 2000 ('RIPA'), as amended and the Codes of Practice issued by the Home Office are carried out effectively and are properly authorised. In addition, it provides guidance to officers and elected members on the requirements and outlines the procedures to be followed in utilising their investigatory powers.

This document should be in conjunction with the legislation and the Home Office's Codes of Practice.

1.2 The activities covered by this policy and guidance document are:

- covert surveillance
- the use of covert human intelligence sources (CHIS)

These investigatory powers should only be used in circumstances where it is necessary and proportionate having considered all the requirements of the legislation, codes of practice and this policy. The legislation and codes should be consulted from time to time, and at annual review to ensure this document remains up to date.

1.3 **What RIPA Does and Does Not Do**

RIPA does:

- Require prior authorisation of directed surveillance.
- Prohibit the council from carrying out intrusive surveillance.
- Require authorisation of the conduct and use of CHIS.
- Require safeguards for the conduct of the use of a CHIS.

RIPA does not:

- Make unlawful conduct which is otherwise lawful.
- Prejudice any existing power to obtain information by any means not involving conduct that may be authorised under RIPA. For example, it does not affect the council's current powers to obtain information via the DVLA or to obtain information from the Land Registry as to the owner of a property.
- Apply to activities outside the scope of Part II of RIPA, which may nevertheless be governed by other legislation, including the HRA. A public authority will only engage RIPA when in performance of its 'core functions' – i.e., the functions specific to that authority as distinct from all public authorities.

1.4 Further guidance on the requirements of the legislation, the codes of practice and this policy can be obtained from the Legal Services team of Walsall Council.

1.5 The requirements of RIPA, as supported by this document, are important for the effective and efficient operation of the Council's actions with regard to Covert Surveillance and Covert Human Intelligence Sources. This policy and procedure document will therefore be kept under annual review by the Executive Director of Economy, Environment & Communities, who is the nominated Senior Responsible Officer (SRO) for the purpose of RIPA. Authorising Officers must bring any suggestions for continuous improvement of this document to the attention of the Executive Director for Economy, Environment & Communities at the earliest opportunity.

1.6 In circumstances where RIPA does not apply, this does not mean that surveillance cannot be undertaken, but it must be carried out with due regard to all legal requirements, giving due attention to the necessity, reasonableness and proportionality tests (and relevant articles of ECHR) see 3.13.

1.7 This policy and guidance document will be considered by Cabinet on an annual basis and this report will include a review of the use of RIPA by the organisation. Where changes are required to the Policy either because of updates to legislation, codes of practice or other guidance; the Policy and details of the use to which it has been put will be considered by Cabinet before progressing for approval and adoption by full Council. Minor amendments to the policy, for example as a result of structural changes within the organisation or adding further Authorising Officers, may be made by the Executive Director Economy, Environment and the Communities during the life of the policy and will be brought to the attention of Cabinet and full Council as part of the annual report.

1.8 **Consequences of Failing to Comply with this Policy**

Where there is interference with Article 8 of the ECHR, and where there is no other source of lawful authority for the interference, the consequences of not following the correct authorisation procedure set out under RIPA and this Policy may result in the Council's actions being deemed unlawful. This could in turn lead to claims for compensation, loss of reputation and in certain circumstances any information obtained that could be of help in a prosecution will be inadmissible.

2. Legislative Background

2.1 On 2 October 2000 the Human Rights Act 1998 ("HRA") made it unlawful for a local authority to breach any article of the ECHR. An allegation that the Council or someone acting on behalf of the Council has infringed the ECHR is dealt with by the domestic courts rather than the European Court of Justice.

The ECHR states:

a) individuals have the right to respect for their private and family life, home and correspondence (Article 8 ECHR); and

b) there shall be no interference by a public authority with the exercise of this right unless that interference is:

- in accordance with the law
- necessary and
- proportionate

2.2 RIPA, which came into force on 25 September 2000, provided a lawful basis for three types of investigatory activity to be carried out by local authorities which might otherwise breach the ECHR. The activities were:

a) covert surveillance

b) covert human intelligence sources ("CHIS") and

c) acquisition and disclosure of communications data.

This regime was further refined with the introduction of the Investigatory Powers Act 2016 (IPA). From April 2019, while the first two investigatory techniques above remained within RIPA and are still current, the legislative powers and controls relating to the acquisition and disclosure of communications data moved to the IPA. There is a separate policy within Walsall Council governing the acquisition of communications data under IPA.

2.3 RIPA set outs procedures that must be followed to ensure the activity is lawful. Where properly authorised under RIPA, the activity will be a justifiable interference with an individual's rights under the ECHR; if the interference is not properly authorised an action for breach of the HRA could be taken against the Council, a complaint of maladministration made to the Local Government Ombudsman or a complaint made to the Investigatory Powers Tribunal.

2.4 In addition, if the procedures are not followed any evidence collected may be disallowed by the courts. RIPA seeks to balance the rights of individuals against the public interest in the Council being able to carry out its statutory duties.

3. Surveillance

3.1 Surveillance can be defined as "overt", "covert", "directed" and "intrusive" and includes

- monitoring, observing, listening to persons, watching or following their movements, listening to their conversations and other such activities or communications.
- Recording anything mentioned above in the course of authorised surveillance.
- surveillance, by or with, the assistance of appropriate surveillance device (s).

3.2 **Overt Surveillance**

The majority of the Council's surveillance activity will be overt surveillance i.e., will be carried out openly. For example

- where the Council performs regulatory checks on licensees to ensure they are complying with the terms of any licence granted

- where the Council advises a resident that their activities will be monitored as a result of neighbour nuisance allegations
- or where an officer uses body worn cameras and informs the individual that the camera will be switched on and recording will take place. This type of overt surveillance is normal Council business and is not regulated by RIPA.

3.3 **Covert Surveillance**

This is where surveillance is carried out in a way that ensures that the person subject to the surveillance is unaware it is taking place.

3.4 Where covert surveillance activities are unlikely to result in obtaining of any private information about a person (because the surveillance although covert is general or low level, and is not directed at particular individuals), no interference with Article 8 rights occurs, and an authorisation under RIPA is not required.

3.5 RIPA authorisation may however be required where the surveillance is repeated for a particular purpose and could amount to systematic surveillance of an individual. If in doubt advice should be sought from Legal Services.

3.6 **Covert Directed Surveillance**

Surveillance that is:

- covert
- not intrusive
- for the purposes of a specific investigation or operation
- likely to obtain private information about a person (whether or not that person was the target of the investigation or operation); and
- not carried out as an immediate response to events or circumstances which could not have been foreseen prior to the surveillance taking place

3.7 **Directed Surveillance Crime Threshold**

Following the changes to RIPA introduced by The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012 a crime threshold applies to the authorisation of directed surveillance by local authorities.

3.8 Authorising Officers (AO's) may not authorise directed surveillance unless it is for the purpose of preventing or detecting a criminal offence AND meets the following:

- The criminal offence is punishable by a maximum term of at least 6 months imprisonment, or
- involves the sale of tobacco and alcohol to underage children which is an offence under sections 146, 147, or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1993 (offences).

3.9 **Covert Intrusive Surveillance**

Local authorities cannot lawfully carry out covert intrusive surveillance however to assist in decision making the following section describes what covert intrusive surveillance is.

3.10 Covert intrusive surveillance takes place when covert surveillance is carried out in relation to anything taking place on residential premises or in a private vehicle.

3.11 It also involves the presence of an individual or surveillance device on the premises or in the vehicle, or the use of a device placed outside the premises or vehicle which consistently provides information of the same quality and detail as expected of a device placed inside.

3.12 Additionally, the Regulation of Investigatory Powers (Extension of Authorisations Provisions: Legal Consultations) Order 2010 states that covert surveillance carried out in relation to anything taking place in certain specified premises is intrusive when they are being used for legal consultation.

3.13 Non RIPA Authorisations

3.14 Some activity (and bearing in mind the tests at 3.8) is not classed as directed surveillance and no authorisation is required nor can be given for that activity for example.

- Covert surveillance in immediate response to events. Where officers are carrying out their routine duties and an incident occurs that they decide to follow and it is not reasonably practicable to be expected to obtain an authorisation, then an authorisation is not required.
- Covert surveillance as part of general observation work. Where officers are carrying out routine work, such as walking through town to ensure there are no breaches of legislation which they enforce, monitoring publicly accessible parts of the internet which are not part of a specific investigation, then this is not classed as covert surveillance.
- Covert surveillance not related to the statutory grounds or core activities of the Authority. RIPA authorisation is only required for specific investigations or operations where it is necessary on the grounds specified in s28(3) of the 2000 Act. Covert surveillance carried out for any other purpose should be conducted in accordance with the relevant legislation and RIPA authorisation is not required. RIPA is required for core functions that are specific to that authority, e.g. the work of enforcement teams within the Council.

  General activities that are carried out by all authorities, e.g. employment issues, are classed as ordinary functions and not subject to RIPA. However, other legislation such as the Human Rights Act, General Data Protection Regulations may apply.
- Overt use of CCTV and ANPR systems. CCTV systems are used by the Council in a number of situations and the public are normally made aware that they are in use. RIPA authorisation is not normally required where these systems are used for the general monitoring of the area or to review an incident and gather evidence of a crime after it has happened.

However, where the system is used in a covert manner to monitor a particular subject as part of a planned operation, this becomes directed surveillance and a RIPA authorisation should be obtained.

- Covert surveillance as part of an equipment interference warrant. Where a warrant has been obtained under part 5 of the 2016 Act, then a separate RIPA authorisation is not required.
- Recording equipment worn by a CHIS. Where a CHIS acting under a conduct authorisation wears a recording to record information obtained in their presence a separate RIPA authorisation is not required.
- Covert recording of noise recording sound levels only. A RIPA authorisation is not required where a covert noise recording device records only sound levels; machinery, music or other non-verbal noise; or verbal content is recorded at a level which does not exceed that which can be heard in the street outside or adjoining the property with the naked ear.

3.15 Where investigating Officers are undertaking surveillance examples of which are given above (3.14) should still give consideration to the necessity and proportionality of the surveillance and seek authorisation from an AO to proceed.

3.16 The appropriate 'Application for authorisation to carry out directed surveillance' forms at **APPENDIX 1** should be completed, authorised and stored securely by the relevant AO.

4 Private information

4.1 The 2000 Act states that private information includes any information relating to a person's private or family life. As a result, private information is capable of including any aspect of a person's private or personal relationship with others, such as family and professional or business relationships.

4.2 Private information may include personal data, such as names, telephone numbers and address details. Where such information is acquired by means of covert surveillance of a person having a reasonable expectation of privacy, a directed surveillance authorisation is appropriate.

4.3 Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public may still result in the obtaining of private information. This is likely to be the case where that person has a reasonable expectation of privacy even though acting in public and where a record is being made by a public authority of that person's activities for future consideration or analysis. Surveillance of publicly accessible areas of the internet should be treated in a similar way, recognising that there may be an expectation of privacy over information which is on the internet, particularly when accessing information on social media websites (see 9).

4.4 Private life considerations are particularly likely to arise if several records are to be analysed together in order to establish, for example, a pattern of behaviour, or if one or more pieces of information (whether or not available in the public domain) are covertly (or in some cases overtly) obtained for the purpose of making a permanent record about a person or for subsequent data processing to generate further information. In such circumstances, the totality of information gleaned may constitute private information even if individual records do not. Where such conduct includes covert surveillance, a directed surveillance authorisation may be considered appropriate.

Practical examples of these differing scenarios can be found in the Code of Practice for Covert Surveillance and Property Interference on the Home Office website.

5 Confidential Information

5.1 A higher level of authorisation to apply to the Magistrates Court is required in relation to RIPA activity when the subject of the investigation might reasonably expect a high degree of privacy, or where "confidential information" might be obtained. For the purpose of RIPA this includes:

- communications subject to legal privilege
- communications between a member of parliament and another person on constituency matters
- confidential personal information and
- confidential journalistic material

5.2 The AO and the person carrying out the surveillance must understand that such information is confidential and is subject to a stringent authorisation procedure. Authorisation can only be granted by the Chief Executive or in their absence by an officer acting as Head of Paid Service.

5.3 Any officer contemplating RIPA activity where the above circumstances may apply must seek advice from Legal Services prior to making any application.

6. Covert Human Intelligence Sources ("CHIS")

6.1 The Council is permitted to use CHIS subject to strict compliance with RIPA.

6.2 A CHIS is a person who establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating:

(a) covertly using the relationship to obtain information or provide access to information to another person, or

(b) covertly disclosing information obtained by the use of the relationship or as a consequence of the existence of such a relationship.

6.3 A RIPA authorisation and order from a magistrate is required for the above activity and should be obtained whether the CHIS is a Council officer or another person who is asked to be a CHIS on the Council's behalf. Authorisation for CHIS can only be granted if it is for the purposes of preventing or detecting crime or of preventing disorder.

6.4 Members of the public who volunteer information to the Council and those engaged by the Council to carry out test purchases in the ordinary course of business (i.e., they do not develop a relationship with the shop attendant and do not use covert recording devices) are not CHIS and do not require RIPA authorisation.

6.5 However, by virtue of section 26(8) (c) of RIPA, there may be instances where an individual, who covertly discloses information though not tasked to do so may nevertheless be a CHIS.

6.6 The important question is how did the member of the public acquire the information which they volunteer? If they acquired it in the course of, or as a result of the existence of, a personal or other relationship, they are likely to fall within the definition of a CHIS. If the Council then makes use of the information, and the informant is thereby put at risk, the Council may be in breach of its duty of care owed to the individual. It is recommended that legal advice is sought in any such circumstances.

6.7 The Covert Human Intelligence Sources Code of Practice can be found on the Home Office website.

6.8 The Covert Human Intelligence Sources (Criminal Conduct) Act 2021 (legislation.gov.uk) restricts the authorisation of a CHIS who can carry out criminal conduct to certain organisations. Local authorities are not included within scope of this list. Therefore, Walsall Council will not authorise a CHIS to carry out criminal conduct.

7 Vulnerable Individuals / Juvenile CHIS

7.1 Although it is unlikely Walsall Council would use such persons additional requirements would apply to the use of a vulnerable individual or a person under the age of 18 as a CHIS. In both cases authorisation for an application to the Magistrates Court can only be granted by the Chief Executive or in their absence by an officer acting as Head of Paid Service. Any officer contemplating the use of a juvenile or a vulnerable person as a CHIS must seek advice from Legal Services prior to making the application.

7.2 The use or conduct of a CHIS under 16 years of age must not be authorised to give information against their parents or any person who has parental responsibility for them.

7.3 In other cases authorisations should not be granted unless the special provisions contained in The Regulation of Investigatory Powers (Juveniles) Order 2000 (as amended in 2018) are satisfied. This sets out rules about parental consent, meetings, risk assessments and the duration of the authorisation.

7.4 The Draft Revised Home Office Guidance on Covert Human Intelligence Sources (January 2021) sets out additional guidance on measure to protect a juvenile CHIS. These additional measures are that:

- An appropriate adult is present at any meeting with a CHIS under 16 or 17 years of age
- Where a CHIS is 16 or 17 years of age, consideration should be given to the presence of an appropriate adult. In making this decision, consideration should be given to the maturity of the juvenile and their ability to make an informed decision.
- The appropriate adult should normally be the parent or guardian of the juvenile unless they are unavailable or there are specific reasons for excluding them, e.g. their involvement in the matters under investigation or the juvenile provides a clear reason to exclude them.
- Where the appropriate adult is not the parent or guardian, the person who acts as the appropriate adult should be someone with personal links to the juvenile, or someone who has professional qualifications that enable them to carry out the role, such as a social

worker. The appropriate adult should be someone who is independent of the AUTHORITY.

- A juvenile CHIS should only be approved by the Head of Paid Service or a person acting as Head of Paid Service.

7.5 Although these measures are still in draft form, it is the policy of Walsall MBC to adopt these measures.

7.6 A vulnerable individual is a person who by reason of mental disorder or vulnerability, other disability, age or illness, is or may be unable to take care of themselves or protect themselves against significant harm or exploitation.

8. CCTV

8.1 The installation and use of unconcealed CCTV cameras for the purpose of generally observing activity in a particular area is not surveillance requiring RIPA authorisation. However, there are specific provisions regulating the use of CCTV cameras in public places and buildings and the Council has drawn up a Corporate CCTV Policy which officers must comply with. However, if CCTV cameras are being used in such a way that the definition of covert directed surveillance is satisfied, RIPA authorisation should be obtained.

8.2 For instance the use of town centre CCTV systems to identify those responsible for a criminal act immediately after it happens will not require RIPA authorisation.

However, the use of the same CCTV system to conduct planned surveillance of an individual and record his movements is likely to require authorisation.

8.3 Protocols should be agreed with any external agencies requesting use of the Council's CCTV system. The protocols should ensure that the Council is satisfied that authorisations have been validly granted prior to agreeing that the CCTV system may be used for directed surveillance.

9. Use of Social Media / Internet

9.1 The internet may be utilised to obtain information including viewing specific user profiles on Social Networking Sites ('SNS') or searching SNS to try to find profiles that contain useful information. Used correctly, research of SNS might provide invaluable evidence or at least useful intelligence.

9.2 Some activity on SNS might however constitute Directed Surveillance or require CHIS authorisation, some may not. Similarly, some research might be likely to result in the obtaining of private information, some may not. Activity that does not meet the threshold for RIPA authorisation but might be likely to result in obtaining private information will require consideration of Human Rights issues such as balancing the protection of rights with the breach of privacy, necessity and proportionality.

9.3 It is important to note that images of persons are private information, and also for officers to be aware that it is possible they might obtain private information about other individuals not just the specific user on the profiles which are viewed, captured or recorded. These individuals might not even be aware this private information has been made public by the profile/account holder.

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

9.5 If it is necessary and proportionate for an officer to covertly record information from a SNS, the minimum requirement is an authorisation for directed surveillance.

9.6 An authorisation for the use and conduct of a CHIS is necessary if a relationship is established or maintained by a member of a public authority or by a person acting on its behalf (i.e., the activity is more than mere reading of the site's content). This could occur if an officer covertly asks to become a 'friend' of someone on a SNS and subsequently forms a relationship with them

9.7 Use of an established overt presence of the public authority on the SNS to look at publicly available information on the profile is possible and viable if the Council has a presence on the SNS which is used to publicly and overtly make the presence of the Council known, however this does not mean that information freely displayed on a profile is "fair game".

9.8 The first covert visit to an SNS profile which might be displaying lots of private information could be regarded as a 'drive by' however any subsequent covert visits, particularly on a regular basis are likely to require authorisation for directed surveillance if the Council is likely to obtain private information, and this would be obvious as a result of the initial visit.

9.9 In his annual report for 2020 (published Jan 2022), The investigatory Powers Commissioner recommended that all activity relating to investigations where activity accessing the internet and social networking sites is recorded so that the SRO can monitor such activity to ensure it is being used in a "controlled and well understood manner".

9.10 In Walsall, such activity should already be recorded on the case worksheets for Regulatory Services. To enable better monitoring a new action code has been created against which this activity must be logged. Other services who carry out such activity should record it in a way in which it can be monitored.

10. Aerial Surveillance

10.1 Where surveillance is carried out using aircraft, whether manned, eg helicopters, or unmanned, e.g. drones, or other aerial devices then the same considerations need to be given to whether RIPA authorisation is needed as for any other type of surveillance. Particular consideration needs to be given to the reduced visibility and awareness of the device at height.

11 Residential Premises & Vehicles

11.1 Residential premises are defined as any premises for the time being occupied by any person, including on a temporary basis, for residential purposes or as living accommodation, including hotels. However, common areas to which a person has access in connection with that use are excluded. Residential premises occupied by a local authority for non-residential purposes are excluded. For example, a house covertly used by trading standards to which traders are invited to carry out maintenance work or repair known faults, to discover if they are acting honestly. (A "house of horrors" set up.)

11.2 Examples of locations which are and are not classed as residential premises are given below:

Examples of locations classed as residential premises	Examples of locations not classed as residential premises
Rented flat	Communal stairway in block of flats (unless used as temporary place of abode by a homeless person)
Hotel bedroom or suite	Hotel reception or dining room
	Front garden of premises readily visible to the public
	House of horrors

11.3 **Private vehicles** are defined as a vehicle, including a vessel, aircraft or hovercraft, which is used primarily for the private purposes of the person who owns it or having the right to use it. This includes a company car used for business and pleasure of an employee.

11.4 The use of a tracking or recording device in vehicles owned by a local authority is unlikely to be covert if members of staff are informed of that use. However, if they are used for a purpose that the employee has not been informed of, or for the purpose of covertly monitor, record, observe, listen to the occupants, then that may require authorisation.

12. Restrictions on Certain Activities

12.1 Local Authorities are not permitted within the legislation to undertake certain activities including:

- interference with private property e.g. placing tracking devices on private vehicles
- carrying out surveillance which is intrusive
- interception of communications

12.2 At no time should the Council or any officers undertake any surveillance if it falls within any of these categories. If in doubt seek the advice of the SRO, AO or legal services as soon as practicable.

13. Authorisation Procedures

13.1 Authorising Officers/Designated Persons for directed surveillance and CHIS

Authorising Officers are responsible for assessing and authorising covert directed surveillance and the use of a CHIS.

13.2 It is the responsibility of Authorising Officers to ensure that when applying for authorisation the principles of necessity and proportionality (see 13.9 below) are adequately considered and evidenced; and that reviews and cancellations of authorisations are carried out as required under this Policy.

13.3 A list of AOs is contained at **APPENDIX 2**. Any requests for amendments to the lists must be made in writing and sent to the SRO.

13.4 Schedule 1 of statutory instrument No. 521 (2010) prescribes the rank or position of authorising officers for the purposes of Section 30(1) of RIPA (covert surveillance and CHIS). For Local Authorities they prescribe a "Director, Head of Service, Service Manager or equivalent".

The term Director is not defined within the Act but in Walsall Council it has been determined that it would normally equate to the Executive Director or a member of Corporate Management Team.

13.5 The SRO designates which officers can be AO's. Only these officers can authorise directed surveillance and the use of CHIS. All authorisations must follow the procedures set out in the Policy. AOs are responsible for ensuring that they have received RIPA training prior to authorising RIPA activity. When applying for or authorising RIPA activity under the Policy, officers must also take into account the corporate training and any other guidance issued from time to time by the SRO.

13.6 All forms that are used in the respect of RIPA applications, renewals, reviews or cancellations should be taken from the Home Office website.

https://www.gov.uk/government/collections/ripa-forms--2

13.7 Authorisation of Covert Directed Surveillance and Use of a CHIS

13.8 Whether by Council officers or external agencies engaged by the Council, RIPA applies to all covert directed surveillance and use of CHIS. Council officers wishing to undertake directed surveillance or use of a CHIS must complete the relevant application form and forward it to the relevant authorising officer.

13.9 Directed surveillance and use of a CHIS can only be authorised if the authorising officer is satisfied that the activity is: -

(a) in **accordance with the law** i.e., it must be in relation to matters that are statutory or administrative functions of the Council.

(b) **necessary** for the purpose of preventing or detecting crime or preventing disorder. This is the only ground available to the Council for authorising RIPA activity and there is a crime threshold for directed surveillance as described in paragraph 3.7 above; and

(b) **proportionate** to what it seeks to achieve. This involves balancing the seriousness of the intrusion into the privacy of the subject of the operation (or any other person as may be affected) against the need for the activity in investigative operational terms. Any conduct that is excessive as to the interference and the aim of the conduct, or is in any way arbitrary will not be proportionate. Serious consideration must be given to identifying the least intrusive method of obtaining the information required.

13.10 Officers making a RIPA application should ask the following types of questions to help determine whether the use of RIPA is necessary and proportionate:

- why it is believed the proposed conduct and use is necessary for the prevention of crime or the prevention of disorder (as appropriate)
- how the activity to be authorised is expected to bring a benefit to the investigation
- how and why the proposed conduct and use is proportionate to the intelligence dividend it hopes to achieve, having regard to the gravity and extent of the activity under investigation
- how and why the methods to be adopted will cause the least possible intrusion to the subject/s i.e., interfere with their rights under the ECHR
- what other reasonable methods of obtaining information have been considered and why they have been discounted
- Authorising officers/designated persons should not be responsible for authorising their own activities i.e., those operations/investigations in which they are directly involved. However, it is recognised that in exceptional circumstances this may sometimes be unavoidable.

13.11 Particular consideration should be given to collateral intrusion on or interference with the privacy of persons who are not the subject(s) of the investigation. Collateral intrusion occurs when an officer undertaking covert surveillance on a subject observes or gains information relating to a person who is not the subject of the investigation. An application for an authorisation must include an assessment of the risk of any collateral intrusion or interference and measures must be taken to avoid or minimise it. This must be taken into

account by the authorising officer/designated person, particularly when considering the proportionality of the surveillance.

13.12 Particular care must be taken in cases where confidential information is involved e.g., matters subject to legal privilege; confidential personal information; confidential journalistic material; confidential medical information; and matters relating to religious leaders and their followers. In cases where it is likely that confidential information will be acquired, officers must specifically refer this to Legal Services for advice.

13.13 The activity must be authorised before it takes place. At the time of authorisation, the authorising officer must set a date for review of the authorisation and review it on that date.

13.14 A copy of the completed relevant application and authorisation form must be forwarded to the SRO within one week of the authorisation for example by e-mail as a scanned document. The SRO will maintain a central register of the Council's RIPA activity and a unique reference number will be allocated to each application.

14. The Magistrates Court

14.1 Following changes under the Protection of Freedoms Act 2012, there is an additional stage in the process for the investigatory activities of Directed Surveillance and CHIS. After the Authorisation form has been countersigned by the AO, the Council is required to obtain judicial approval for either the authorisation or a renewal of an authorisation. The role of the Magistrates Court is set out in section 32A RIPA.

14.2 This section provides that the authorisation shall not take effect until the Magistrates Court has made an order approving such authorisation. The matters on which the Magistrates Court needs to be satisfied before giving judicial approval are that:

- There were reasonable grounds for the local authority to believe that the authorisation or notice was necessary and proportionate
- In the case of a CHIS authorisation, that there were reasonable grounds for the local authority to believe that:
    - arrangements exist for the safety and welfare of the source that satisfy section 29(5) RIPA;
    - the requirements imposed by Regulation of Investigatory Powers (Juveniles) Order 2000 were satisfied;
- The local authority application has been authorised by an authorising officer or designated person (as appropriate)

14.3 In cases where there is collaborative working with another agency, for example, the Police, as part of a single investigation or operation, only one authorisation from one organisation is required. This should be made by the lead authority of that particular investigation. Duplication of authorisation does not affect the lawfulness of the investigation or operation but could create an unnecessary administrative burden. Where the Council is not the lead authority in the circumstances, Council officers should satisfy themselves that authorisation has been obtained, and what activity has been authorised.

14.4 The grant of the authorisation was not in breach of any restriction imposed by virtue of an order made under the following sections of RIPA:

15 29(7)(a) (for CHIS),
16 30(3) (for directed surveillance and CHIS)

14.5 It should be noted that only the initial authorisation and any renewal of the authorisation require magistrates' approval.

14.6 There is no requirement for officers presenting authorisations to the Magistrates Court to be legally qualified.

15. The procedure for applying for directed surveillance or use of a CHIS.

- Applicant officer completes an application
- Authorisation is sought from the Authorising Officer
- Applicant officer creates court pack
- Applicant officer proceeds to court
- Applicant officer organises the directed surveillance or use of a CHIS to take place
- Applicant provides the SRO with updated paperwork relating to reviews, renewals or cancellations

At any stage and particularly for inexperienced staff or potentially contentious investigations advice from Legal Services ought to be sought.

16. **Additional Requirements for Authorisation of a CHIS**

16.1 A CHIS must only be authorised if the following arrangements are in place:

- there is a Council officer with day-to-day responsibility for dealing with the CHIS (CHIS handler) and a senior council officer with oversight of the use made of the CHIS (CHIS controller);
- a risk assessment has been undertaken to take account of the CHIS security and welfare
- a Council officer is responsible for maintaining a record of the use made of the CHIS
- any adverse impact on community confidence or safety regarding the use of a CHIS has been considered taking account of any particular sensitivities in the local community where the CHIS is operating and
- records containing the identity of the CHIS will be maintained in such a way as to preserve the confidentiality or prevent disclosure of the identity of the CHIS

17. Urgent Authorisations

17.1 By virtue of the fact that an authorisation under RIPA is not approved until signed off by a Magistrate, urgent oral authorisations are no longer available.

18. Review of Authorisations

18.1 AOs must make arrangements to periodically review any authorised RIPA activity.

18.2 Officers carrying out RIPA activity or external agencies engaged by the Council to carry out RIPA activity must periodically review it and report back to the authorising officer if there is any doubt as to whether it should continue. For Juvenile CHIS's, the Code of Practice stipulates that the authorisation should be reviewed on a monthly basis. Reviews should be recorded on the appropriate Home Office form.

18.3 A copy of the Council's notice of review of an authorisation must be sent to the SRO within one week of the review to enable the central record on RIPA to be authorised.

19 Renewal of Authorisations

19.1 If the AO considers it necessary for an authorisation to continue they may renew it for a further period, beginning with the day when the authorisation would have expired but for the renewal. They must consider the matter again taking into account the content and value of the investigation and the information so far obtained.

Renewed authorisations will normally be for a period of

1. up to 3 months for covert directed surveillance,
2. 12 months in the case of CHIS,
3. 4 months in the case of juvenile CHIS

Authorisations may be renewed more than once, provided they are considered again and continue to meet the criteria for authorisation.

19.2 Applications for the renewal of an authorisation for covert directed surveillance or CHIS authorisation must be made on the appropriate form. The reasoning for seeking renewal of a RIPA notice should be set out by the applicant in an addendum to the application form which granted the initial authorisation.

19.3 All renewals will require an order of the Magistrates Court.

20 Cancellation of Authorisations

20.1 The person who granted or last renewed the authorisation must cancel it when they are satisfied that the covert directed surveillance or CHIS authorisation is no longer meets the criteria for authorisation. Cancellations must be made on the appropriate form.

20.2 Where necessary and practicable, the safety and welfare of the CHIS should continue to be taken into account after the authorisation has been cancelled, and all welfare matters are addressed.

20.3 A copy of the Council's notice of cancellation of an authorisation must be sent the SRO within one week of the cancellation to enable the central record on RIPA to be updated.

21. What happens if the surveillance has unexpected results?

21.1 Those carrying out the covert surveillance should inform the authorising officer if the investigation unexpectedly interferes with the privacy of individuals who are not the original subjects of the investigation or covered by the authorisation.
In some cases, the original authorisation may not be sufficient to cover the activity required or information likely to be gathered and in such cases, consideration should be given as to whether a separate authorisation is required.

22 Errors

22.1 Proper application of the RIPA provisions, and robust technical systems, should reduce the scope for making errors. At Walsall Council the SRO will undertake a regular review of errors and a written record will be made of each review.

22.2 An error may be reported if it is a "relevant error". Under section 231(9) of the Investigatory Powers Act 2016, a relevant error is an error by a public authority in complying with any requirements that are imposed on it by an enactment, such as RIPA, which is subject to review by a Judicial Commissioner.

22.3 Examples of a relevant error include where surveillance or CHIS activity has taken place without lawful authorisation, and/or without adherence to the safeguards set out within the relevant statutory provisions or the relevant Home Office Codes of Practice.

22.4 Where a relevant error has been identified, the Council should notify the Investigatory Powers Commissioner (IPCO) as soon as reasonably practical, and no later than 10 working days (unless otherwise agreed by IPCO). The process for informing IPCO is set out in the relevant Home Office Codes of Practice.

23. Records of RIPA Authorisations

23.1 There will be a central record of RIPA authorisations which is maintained by the SRO. The central record will contain the following information:

- the type of authorisation
- the date it was given
- the name and position of the AO
- the unique reference number of the investigation or operation
- the title of the investigation or operation, including a brief description and names of the subjects, if known
- the date of attending the magistrates court

- the determining magistrate
- the decision of the court
- the date and time of that decision
- the dates of any reviews
- the date of any renewal
- the AO for the renewal
- judicial information relating to any renewal
- whether the activity is likely to result in obtaining confidential or privileged information
- whether the authorisation was granted by a person directly involved in the investigation
- the date the authorisation was cancelled

23.2 In addition, the following information will also be retained by the SRO in a central file:

- a copy of the application and authorisation along with any additional supporting documentation and any notification of approval given by the AO
- a record of the period over which the surveillance took place
- the frequency of reviews prescribed by the AO and a copy of the record of those reviews
- a copy of any renewal authorisation together with any supporting documentation
- the date and time when any instruction to cease surveillance was given by the AO
- the date and time when any other instruction was given by the AO
- a copy of the order approving or otherwise the grant or renewal of an authorisation from a Justice of the Peace.
- The officer making the application will be responsible for making sure that copies the original papers are given to that person as soon as practicable after each document is signed.
- The central record and copies of documents shall be maintained for seven years and provided to the Investigatory Powers Commissioner on request.

23.3 These records may be digital records only, provided they are a true record of the original documentation and are centrally available.

24. Handling of Material and Safeguards

24.1 When surveillance is carried out, information about the subject of the surveillance will be obtained. This may include information which an officer has observed and recorded, written communications, records, photographic and video images. There may also be information

gathered about other persons (collateral intrusion). All such information is referred to here as material. As well as the legislation governing RIPA, due regard must also be given to data protection legislation and the Authority's policies thereunder to ensure that the handling of private information continues to be lawful, justified and strictly controlled and is subject to robust and effective safeguards.

24.2 Any breaches of the safeguards which are in place to protect material must be investigated. A record of the investigation, conclusion and corrective actions is to be made and reported to the IPCO. Where appropriate, the Information Commissioner must also be notified.

24.3 Material should only be copied, retained and disseminated to the minimum degree necessary for authorised purposes, namely:

- the material is, or is likely to become, necessary for any of the statutory purposes set out in the 2000, 1997 or 1994 Acts in relation to covert surveillance
- the material is necessary for carrying out the functions of the Authority
- the material is necessary for carrying out the functions of the IPC or the Investigatory Powers Tribunal
- the material is necessary for legal proceedings
- the material is necessary for the performance of the functions of any person by or under any enactment.

24.4 Material obtained may be used to further investigations where it is necessary and provided that the safeguards are followed.

25. Use of Material as Evidence

25.1 Material obtained may be used as evidence in criminal proceedings.

25.2 Ensuring the continuity and integrity of evidence is important and governed by other legislation. Material obtained as a result of covert surveillance is also subject to the disclosure rules of the Criminal Procedure and Investigations Act 1996 and its associated codes of practice. Particular attention needs to be paid to the requirement to disclose all material obtained during the course of an investigation which may be relevant to the investigation when making an application for RIPA and in carrying out and recording information during the course of surveillance.

26. Disseminating Material

26.1 It is necessary to share information internally within the Authority and with external organisations such as other local authorities, the police and oversight organisations. This must be limited to the minimum necessary for the authorised purposes of the investigation or functions of the relevant organisation. This includes restricting dissemination within the Authority to only those persons who have a bona fide need to know the information. The amount of material disclosed should be the minimum necessary, including where relevant

providing only a summary of the material.

26.2 Where material is disseminated outside the organisation, similar provisions will apply. The restrictions on further dissemination should be explicitly outlined in writing including, where relevant, the need to obtain written permission before disseminating the material further.

26.3 Material should not be disseminated to bodies outside the UK without ensuring that they have appropriate safeguards in place. The AO should be consulted before material is disseminated to bodies outside the UK.

27. Copying Material

27.1 Material, including extracts and summaries of it should only be copied to the minimum extent necessary for the authorised purposes. This also applies to any record which refers to the covert surveillance and the identities of any person to whom the material related.

28. Storage of Material

28.1 All material, copies, summaries and extracts of it must be stored to ensure no persons can access it without the proper authority. It must be stored to minimise the risk of loss or theft. Any person handling the material must adhere to this requirement. Measures in place to protect the material include:

- physical security – storage to be in buildings, rooms and cupboards etc where access is restricted

- IT security to restrict access – storage is to be on shared servers, networks, databases etc where access is restricted to only those persons who need access to enable the material to be processed; to further the investigation or authorised purpose or to fulfil the functions of the legislation or this policy.

29. Retention and Destruction of Material

29.1 Where material is retained for an authorised purpose, it will be retained in accordance with the relevant retention policy. E.g. where material is retained for a prosecution, it will be retained in accordance with the document retention policy for prosecutions. The material, including and copies, extracts or summaries should then be destroyed in a secure manner at the end of that period. Where material is not retained for one of the authorised purposes, then it should be destroyed in a secure matter as soon as it the need for retaining it is no longer relevant.

30 Surveillance products

30.1 Where the product of surveillance could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with established disclosure requirements for a suitable further period, commensurate to any subsequent review.

30.2 Particular attention is drawn to the requirements of the Code of Practice issued under the Criminal Procedure and Investigations Act 1996. This requires that material which is obtained in the course of a criminal investigation and which may be relevant to the

investigation must be recorded and retained.

30.3 There is nothing in RIPA which prevents material obtained from properly authorised surveillance from being used in other investigations. The Council will ensure that adequate arrangements are in place for the handling and storage of material obtained through the use of covert surveillance to facilitate its use in other investigations.

30.4 Material obtained through the use of directed surveillance or CHIS containing personal information will be protected by the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA). In addition to the considerations above, material obtained must be used, stored and destroyed in compliance with any other legal requirements, including confidentiality, and the Council's Data Protection, Information Security and Records Management Policies available on the intranet at the Protecting Information pages.

31. Training & Advice and Departmental policies, procedures and codes of conduct

31.1 The SRO will arrange regular training on RIPA. All authorising officers; designated persons and investigating officers should attend at least one session every two years and further sessions as and when required. Training can be arranged on request and requests should be made to the SRO. In particular training should be requested for new starters within the Council who may be involved in relevant activities.

31.2 Where in practice, departments have any policy, procedures or codes of practice in relation to RIPA that are different from or in addition to this Code, they must immediately seek advice from the Legal Services or the SRO.

32. Complaints

32.1 Any person who believes they have been adversely affected by surveillance activity by or on behalf of the Council may complain to the SRO.

They may also complain to the Investigatory Powers Tribunal at:

Investigatory Powers Tribunal
PO Box 33220
London
SW1H 9ZQ

Or via the website

https://www.ipt-uk.com/content.asp?id=28

Appendix 1 Non RIPA Authorisations

Walsall Council

APPLICATION FOR AUTHORISATION TO CARRY OUT DIRECTED SURVEILLANCE
THIS IS NOT A RIPA AUTHORISATION FORM
THIS FORM SHOULD NOT BE USED FOR AUTHORISING RIPA SURVEILLANCE

Public Authority *(including address)*	Walsall Council Civic Centre Darwall Street Walsall WS1 1TP

Name of Applicant		**Unit/Branch/ Division**	
Full address			
Contact Details	Address Tel		
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
Has a pre-surveillance risk assessment been carried out? Yes☐ No☐

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.

5. Explain the information that it is desired to obtain as a result of the directed surveillance.
6. Identify <u>why</u> surveillance is necessary in this particular case:

7. Explain <u>why</u> this directed surveillance is necessary in this particular case:

8. Supply details of any potential collateral intrusion and why the intrusion is unavoidable. 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?

10. Confidential Information. [Code paragraphs 3.1 to 3.12] INDICATE THE LIELIHOOD 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 as follows:

	Response	**Initials**
Why is authorised to conduct surveillance:		
What is authorised for the surveillance:		
Where is it to take place and for how long:		
Why it is being authorised:		
How will the surveillance be conducted:		

This written authorisation will cease to have effect at the end of a period of 3 months unless renewed (see separate form for renewals).

The Applicant and Authorised Officer will jointly review this authorisation on the date below to see whether authorisation should continue, be renewed or cancelled.

13. Authorised Officers statement explaining <u>why</u> in his / her view the directed surveillance is <u>necessary</u> and <u>proportionate</u>. This box must be completed and both aspects must be addressed.

14. (Confidential Information Authorisation.) Supply detail demonstrating compliance with Home Office Codes of Practice relating to this issue.	
Expiry of authorisation (3 months from the date / time of authorisation unless otherwise stated here)	
Programme for subsequent reviews of this authorisation: Only complete this box if review dates after first review are known. If not or inappropriate to set additional review dates then leave blank.	

Authorising Officer Name (Print)		**Job Title**	
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 Authorising officer to explain why they considered the case so urgent that an oral instead of written authorisation was given.				
Name (Print)		**Job Title:**		
Signature		**Date and Time**		
Urgent authorisation Expiry date:		**Expiry time:**		

Remember the 72 hour rule for urgent authorities	e.g. authorisation granted at 5pm on June 1st expires 4.59 on 4th June		

A COPY OF THIS FORM, ONCE IT HAS BEEN AUTHORISED OR REFUSED, MUST BE HELD ON THE INVESTIGATING OFFICER'S FILE

THERE IS NO REQUIREMENT TO PLACE A COPY OF THE AUTHORISATION ON THE CORPORATE DATABASE

Walsall Council

Review of a Directed Surveillance authorisation

REVIEW OF DIRECTED SURVEILLANCE AUTHORISAION
THIS IS NOT A RIPA REVIEW FORM
THIS FORM SHOULD NOT BE USED FOR REVIEWING RIPA SURVEILLANCE

Public Authority *(including address)*	

Applicant		**Unit/Branch/ Division**	
Full address			
Contact Details			
Operation Name		**Operation Number*** *Filing Ref	
Date of authorisation or last renewal		**Expiry date of authorisation or last renewal**	
Review Number			

Details of review:

1. Review number and dates of any previous reviews.	
Review Number	**Date**

2. Summary of the investigation / operation to date, including what private information has been obtained and the value of the information so far obtained.

3. Detail the reasons why it is necessary to continue with the directed surveillance.

4. Explain how the proposed activity is still proportionate to what it seeks to achieve.

5. Detail any incident of collateral intrusion and the likelihood of any further incidents of collateral intrusions occurring.

6. Give details of any confidential information acquired or accessed and the likelihood of acquiring confidential information.

7. Applicant's Details			
Name (Print)		**Tel No.**	
Job Title		**Date**	
Signature			

8. Review Officer's Comments, including whether or not the directed surveillance should continue.

9. Authorising Officer's Statement	
I, [insert name], hereby agree that the directed surveillance investigation/operation as detailed above [should/should not] continue until its next [until its next review/renewal] [should be cancelled immediately].	
Name (Print)	**Job Title**
Signature	**Date**

10. Date of next review.	

A COPY OF THIS FORM, ONCE IT HAS BEEN AUTHORISED OR REFUSED, MUST BE HELD ON THE INVESTIGATING OFFICER'S FILE

THERE IS NO REQUIREMENT TO PLACE A COPY OF THE AUTHORISATION ON THE CORPORATE DATABASE

Walsall Council

APPLICATION FOR RENEWAL OF A DIRECTED SURVEILLANCE

(PLEASE ATTACH A COPY OF THE ORIGINAL AUTHORISATION)
THIS IS NOT A RIPA RENEWAL FORM
THIS FORM SHOULD NOT BE USED FOR AUTHORISING RIPA RENEWALS

Public Authority *(including address)*	

Name of Applicant		**Unit/Branch/ Division**	
Full address			
Contact Details			
Investigation/Operation Name (if applicable)			
Renewal Number			

Details of renewal:

1. Renewal numbers and dates of any previous renewals.	
Renewal Number	**Date**

2. Detail any significant changes to the information as listed in the original authorisation as it applies at the time of renewal.

3. Detail the reasons why it is necessary to continue with the directed surveillance.

4. Detail why the directed surveillance is still proportionate to what it seeks to achieve.

5.Indicate the content and value to the investigation or operation of the information so far obtained by the directed surveillance.

6. Give details of the regular reviews of the investigation or operation.

7. Applicant's Details			
Name (Print)		**Tel No.**	
Grade / Rank		**Date**	
Signature			

8. Authorising Officer's Comments. <u>This box must be completed.</u>

9. Authorising Officer's Statement
I, [insert name], hereby authorise renewal of the directed surveillance/operation as detailed above. The renewal of this authorisation will last for 3 months unless renewed in writing. This authorisation will be reviewed frequently to assess the need for the authorisation to continue.
Name (Print) **Job Title**
Signature **Date**

Renewal From:	Time:	Date:

Date of first review.	
Date of subsequent reviews for this authorisation.	

A COPY OF THIS FORM, ONCE IT HAS BEEN AUTHORISED OR REFUSED, MUST BE HELD ON THE INVESTIGATING OFFICER'S FILE

THERE IS NO REQUIREMENT TO PLACE A COPY OF THE AUTHORISATION ON THE CORPORATE DATABASE

Walsall Council

CANCELLATION OF A DIRECTED SURVEILLANCE AUTHORISATION
THIS IS NOT A RIPA AUTHORISATION FORM
THIS FORM SHOULD NOT BE USED FOR AUTHORISING RIPA SURVEILLANCE

Public Authority (including full address)	

Name of Applicant **Full Address** **Contact Details** **Investigation/Operation Name (if applicable)**	

Details of cancellation:

1. Explain the reason(s) for the cancellation of the authorisation:

2. Explain the value of surveillance in the operation:

3. Authorising Officer's statement:	
I [insert name], hereby authorise the cancellation of the directed surveillance/operation as detailed above.	
Name (Print)	**Job Title**
Signature	**Date**

4. Time and Date of when the authorising officer instructed the surveillance to cease:			
Date:		**Time:**	

5. Authorisation cancelled.	**Date:**	**Time:**

A COPY OF THIS FORM, ONCE IT HAS BEEN AUTHORISED OR REFUSED, MUST BE HELD ON THE INVESTIGATING OFFICER'S FILE

THERE IS NO REQUIREMENT TO PLACE A COPY OF THE AUTHORISATION ON THE CORPORATE DATABASE

APPENDIX 2 List of Authorised Officer Posts for Authorising Directed Surveillance

Post & Post Holder	Scope of Authorisation
Tony Cox Head of Law	Applications for miscellaneous and any application in an urgent situation or absence of primary authorising officer as listed below except for authorising applications for juvenile and vulnerable persons to act as a CHIS Applications pertaining to a non-criminal investigation into the conduct of an employee (non RIPA)
Simon Neilson Executive Director Economy & Environment	Applications from Regulatory Services and Safer Walsall Borough Partnership – where the council is the lead agency Applications for covert human intelligence source (CHIS) except in the case of juvenile / vulnerable adults in which case Annex A of the relevant Home Office Codes of Practice apply.
Dr Helen Paterson Chief Executive	Applications for covert human intelligence source (CHIS) where the CHIS is a juvenile / vulnerable adults. In her absence, this can be a person acting as the Head of Paid Service.
All EDs	Applications for covert human intelligence source (CHIS) where the CHIS is a juvenile / vulnerable adults ONLY IN THE ABSENCE OF THE CHIEF EXECUTIVE
David Elrington Head of Community Safety and Enforcement	Applications from Regulatory Services and Safer Walsall Borough Partnership – where the council is the lead agency Applications for covert human intelligence source (CHIS) except in the case of juvenile / vulnerable adults in which case Annex A of the relevant Home Office Codes of Practice apply.

In the absence of any post holder, this function is delegated to another trained AO, not to a person acting for the post holder. In the case of an approval of an

application for a CHIS who is a juvenile / vulnerable person, this role is restricted to the Head of Paid service, or in their absence a person acting as head of paid service.

Appendix 3 Legislation

The Regulation of Investigatory Powers Act 2000
http://www.legislation.gov.uk/ukpga/2000/23/contents

The Protection of Freedoms Act 2012
http://www.legislation.gov.uk/ukpga/2012/9/contents/enacted

The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012, SI 2012/1500
http://www.legislation.gov.uk/uksi/2012/1500/made

The Human Rights Act 1998
http://www.legislation.gov.uk/ukpga/1998/42/contents

The Data Retention and Acquisition Regulations 2018
http://www.legislation.gov.uk/uksi/2018/1123/contents/made

Covert Human Intelligence Sources (Criminal Conduct) Act 2021 (legislation.gov.uk)

Home Office Revised Code of Practice on Covert Surveillance and Property Interference August 2018 CHIS Code (publishing.service.gov.uk)

Home Office Revised Code of Practice on Covert Human Intelligence Sources August 2018 CHIS Code (publishing.service.gov.uk)