Regulation of Investigatory Powers Act 2000 (“RIPA”) and the Investigatory Powers Act 2016 (“IPA”)

Policy and Procedure

Page left intentionally blank

Contents

1. Abbreviations

CCTV	Closed Circuit Television
CSP	Communications Service Provider
Council	Walsall Council
CHIS	Covert Human Intelligence Sources
DPA	Data Protection Act 2018
ECHR	European Convention for the Protection of Human Rights and Fundamental Freedom agreed on 2 November 1950
HRA	Human Rights Act 1998
IPA	Investigatory Powers Act 2016
IPCO	The Investigatory Powers Commissioner's Office
NAFN	The National Anti-Fraud Network
OCDA	The Office for Communications Data Authorisations
PFA	Protection of Freedoms Act 2012
RIPA	Regulation of Investigatory Powers Act 2000
SPoCs	Single Points of Contact for acquisition and disclosure of communications data

2. Introduction

2.1 This Policy & Procedures document (the Policy) is based upon the requirements of the Regulation of Investigatory Powers Act 2000 (RIPA), the Investigatory Powers Act 2016 (IPA), the Home Office Codes of Practice on Covert Surveillance and Property Interference, Covert Human Intelligence Sources and Acquisition and Disclosure of Communications Data.

2.2 The use of covert surveillance, covert human intelligence sources and the acquisition of service user or subscriber information in relation to communications data is sometimes necessary to ensure effective investigation and enforcement of the law. However, they should be used only rarely and in exceptional circumstances. RIPA requires that public authorities follow a clear authorisation process prior to using these powers. Authorisations granted under Part II of RIPA are subject to all the existing safeguards considered necessary by Parliament to ensure that investigatory powers are exercised compatibly with the ECHR.

2.3 The objective of this policy and procedure is to ensure that all investigations 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.

2.4 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.

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

3. Consequences of Failing to Comply with this Policy

3.1 Consequences of failing to comply with this policy where there is interference with the right to private and family life, home and correspondence under Article 8 of the ECHR, as incorporated in the Human Rights Act 1998, 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 (or IPA) and this Policy may result in the council's actions being deemed unlawful by the courts under Section 6 of the HRA or by the Investigatory Powers Tribunal. This may open-up the council to claims for compensation and loss of reputation.

3.2 Additionally, any information obtained that could be of help in a prosecution will be inadmissible.

3.3 Any queries or concerns relating to RIPA or obtaining communications data should be referred to the Legal Services or the SRO for preliminary advice at the earliest possible opportunity.

4. Background

4.1 On 2 October 2000, the Human Rights Act 1998 ("HRA") made it unlawful for a local authority to breach any article of the ECHR.

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

4.2 RIPA, which came into force on 25 September 2000, provides a lawful basis for two types of investigatory activity to be carried out by local authorities which might otherwise breach the ECHR.

The activities are:
- covert directed surveillance
- covert human intelligence sources ("CHIS")

4.3 Since May 2019, the Investigatory Powers Act 2016 (IPA) provides a lawful basis for local authorities to acquire communications data which was previously obtained through RIPA.

4.4 RIPA and IPA set out procedures that must be followed to ensure the RIPA and obtaining communications data activity is lawful. Where properly authorised

under RIPA or IPA 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 and Social Care Ombudsman or a complaint made to the Investigatory Powers Tribunal. In addition, if the procedures are not followed any evidence collected may be disallowed by the courts. RIPA and IPA seek to balance the rights of individuals against the public interest in the Council being able to carry out its statutory duties.

4.5 **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.
- Apply where covert surveillance is carried out as part of an immediate response to events where it is not reasonably practical to obtain a RIPA authorisation.
- Apply to general observation activities that is unlikely to result in obtaining of any private information about a person or is not directed at particular individuals.

4.6 **What IPA Does and Does Not do**

IPA does:

- Permit the council to obtain specific types of communications records from communications service providers.
- Compel disclosure of specific types of communications data from telecom and postal service providers.

IPA does not:

- permit the council to intercept the content of any person's communication, and it is an offence to do so without any other form of lawful authority
- permit the council to obtain internet connection data.

Further information about the types of communication data the council can obtain can be found at 13.2.

A list of pertinent legislation is contained at **Appendix 3**

4.7 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 (AOs) 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.

4.8 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.

4.9 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 AOs, 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.

5. Policy Statement

5.1 The council is determined to act responsibly and in accordance with the law. All staff who are considering undertaking RIPA activity should be aware that where that activity may involve handling confidential information or the use of vulnerable or juvenile persons as sources of information, a higher level of authorisation is required. Please see 8 (in respect of handling confidential information) and 9 and 10 (in respect of using information sources who are vulnerable or juvenile persons) below.

5.2 The Executive Director Economy, Environment and Communities is the council's Senior Responsible Officer (SRO) and is responsible for the following roles:

- Appointing RIPA AOs
- Appointing Approved Rank Officers for Communications Data
- Maintaining a central record of all RIPA and Communication Data authorisations
- Arranging training to individuals appointed as AOs and Approved Rank Officers, and

- Carrying out an overall monitoring function as the SRO for the council's use of RIPA and IPA powers.

Any officer who is unsure about any RIPA activity or the acquisition or disclosure of Communications Data should contact either the SRO, a relevant AO or Legal Services for advice and assistance.

6. Types of Surveillance

6.1 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).

Overt Surveillance

6.2 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.

Covert Surveillance

6.3 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.

6.4 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.

6.5 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.

Covert Directed Surveillance

6.6 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

Directed Surveillance Crime Threshold

6.7 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.

6.8 Walsall Council AOs 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).

The RIPA Crime threshold only applies to Directed Surveillance, not to CHIS or Communications Data. The Home Office Code of Practice for covert surveillance can be found on the Home Office website at

Covert surveillance code of practice - GOV.UK (www.gov.uk)

Where covert surveillance is required but does not meet the RIPA crime threshold, a non-RIPA directed surveillance application may be made. For further details about surveillance outside of RIPA, please see 6.10.

Covert Intrusive Surveillance

6.9 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 and which involves the presence of an individual or surveillance device on the premises or in the vehicle, or which uses 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. 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.

Non RIPA Authorisations

6.10 Some activity 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.

6.11 Where investigating officers are undertaking surveillance, they should still give consideration to the necessity and proportionality of the surveillance and seek authorisation from an AO to proceed.

6.12 The appropriate 'Application for authorisation to carry out directed surveillance' forms at **Appendix 2** should be completed, authorised and stored securely by the relevant AO.

7 Private information

7.1 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.

7.2 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.

7.3 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 14).

7.4 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.

8 Confidential Information

8.1 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[1]
- communications between a member of parliament and another person on constituency matters
- confidential personal information[2] and

- confidential journalistic material[3]

[1] Legal privilege is defined in section 98 of the Police Act 1997 as:

- communications between a professional legal adviser and his client, or any person representing his client which are made in connection with the giving of legal advice to the client.
- communications between a professional legal adviser and his client or any person representing his client, or between a professional legal adviser or his client or any such representative and any other person which are made in connection with or in contemplation of legal proceedings and for the purposes of such proceedings.
- items enclosed with or referred to in communications of the kind mentioned above and made in connection with the giving of legal advice, or in connection with or in contemplation of legal proceedings and for the purposes of such proceedings.

Communications and items are not matters subject to legal privilege when they are in the possession of a person who is not entitled to possession of them, and communications and items held, or oral communications made, with the intention of furthering a criminal purpose are not matters subject to legal privilege.

If advice is required on this point, officers should contact the Legal Services.

- [2]Confidential personal information is described at paragraph 9.29 of the Home Office Covert Surveillance and Property Interference Revised Code of Practice.
- [3]Confidential journalistic material is described at paragraph 9.38 of the Home Office Covert Surveillance and Property Interference Revised Code of Practice.

8.2 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.

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

9. Covert Human Intelligence Sources ("CHIS")

9.1 The council is permitted to use CHIS subject to strict compliance with RIPA.

9.2 Under the 2000 Act, a person is a CHIS if:

- they establish or maintain a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within Section 26(8)(b) or (c);
- they covertly use such a relationship to obtain information or to provide access to any information to another person; or
- they covertly disclose information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

9.3 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.

9.4 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.

9.5 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. 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.

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

9.7 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.

10 Vulnerable Individuals[5] /Juvenile CHIS

10.1 The Investigatory Powers Commissioner must be informed within seven working days of a CHIS authorisation of a vulnerable adult or a juvenile source. The Investigatory Powers Commissioner intends to keep such authorisations under close review and will report any relevant findings in his annual report.

10.2 Special safeguards apply to the authorisation of a vulnerable adult as a CHIS. A vulnerable adult is a person aged 18 or over who by reason of mental disorder or vulnerability, other disability, age, or illness, is or may be unable to take care of themselves, or unable to protect themselves against significant harm or exploitation. Where it is known or suspected that an adult may be vulnerable, they should only be authorised to act as a CHIS in exceptional circumstances.

10.3 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.

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

10.5 Any officer contemplating the use of a juvenile or a vulnerable person as a CHIS must seek advice from the City Solicitor or the Democratic Services Legal

Team prior to making the application. 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.

[5]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.

11. CCTV

11.1 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 see **Appendix 5**. 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.

11.2 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.

11.3 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.

12. Aerial Surveillance

12.1 Where surveillance is carried out using aircraft, whether manned, e.g. 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.

Acquisition and Disclosure of Communications Data

Communication Service Providers ("CSPs")

13.1 CSPs are organisations that are involved in the provision, delivery and maintenance of communications such as postal, telecommunication and internet service providers but also, for example, hotel or library staff involved in providing and maintaining e-mail access to customers. The Council must obtain communications data from CSPs in strict compliance with IPA.

Types of Communications Data

13.2 Sections 261 and 262 IPA 2016 provide the definitions of communications data, telecommunications, postal services and systems.

13.3 Communications data is the 'who', 'where', 'when' and 'how' of a communication such as a letter, phone call or e-mail but not the content, not what was said or written. The council is not able to authorise the interception or acquisition of the content of communications.

13.4 Postal Data is anything comprised in or attached to a communication for the purpose of a postal service, for example addresses or markings of the sender or the recipient either in writing or through online tracking.

13.5 Telecommunications data are all communications data held by a telecommunications operator or obtainable from a telecommunications system.

Previously under RIPA the categories of telecommunication data were "traffic data", "service user data" and "subscriber data". These have been replaced under IPA with two types of telecommunication data:

Entity Data- this is data about entities or links between individuals and devices. Entities can be individuals, groups and objects such as mobile phones, tablets or other communication devices.

Entity data broadly replaces "subscriber data" under RIPA, and may include:

- names and addresses of subscribers, email or telephone account holders as well as payments made;
- make and model of the device used;
- the connection, disconnection and reconnection of services an individual has subscribed to or may have subscribed to.

Entity data describes or identifies how individuals are linked to devices but does not include information about individual events.

Events Data - this is more intrusive; it identifies or describes events which consist of one or more entities, such as individuals engaging in an activity at a specific point (or specific points) in time.
Events data may include:

- call records
- location of a mobile phone
- information which identifies the sender or recipient from data held in the communication
- timing and duration of a call

Events data does not include non-communication events such as a change in address or telephone number.

A basic example of the difference between entity and events data is where a subscriber check is required, such as requiring information about who is the subscriber for mobile number 07999 123456. This would be entity data but if further information is required about the date/time a phone call was made, location or the duration, this would be classed as events data. Obtaining events data requires a higher threshold than for entity data. Further information about this can be found at paragraph 15.32.

The Communications Data Code of Practice contains a non-exhaustive list of examples of events data or entity data. If an applicant is unsure of the category of data they are seeking (entity or events data), or other information relating to telecommunications or postal systems covered under IPA, the applicant should discuss this with their Single Point of Contact (SPoC) or contact the Democratic Services Legal Team for advice.

13.6 The council is not permitted to make an application that requires the processing or disclosure of internet connection records for any purpose.

13.7 The council is not able to intercept or obtain the content of communications in any circumstances, for example the details contained within an email, text message or voicemail.

13.8 Legal basis for Communications Data Authorisation and Notices

IPA provides for acquisition and disclosure of communications data by local authorities only for the prevention and detection of crime or disorder as set out in s73 and s60A IPA 2016. As such the council is unable to access communications data for investigations that are not for the purpose of prevention and detection of crime, for example for civil action or internal employee disciplinary matters.

13.9 Obtaining events data must, in addition, be for serious crime defined in section 86(2A) IPA 2016 as:

- An offence for which an adult is capable of being sentenced to one year or more in prison.
- Any offence involving violence, resulting in a substantial financial gain or involving conduct by a large group of persons in pursuit of a common goal.
- Any offence committed by a body corporate, or;
- Any offence which involves, as an integral part of it the sending of a communication or a breach of privacy.

Care should be taken that the appropriate lawful requirements for the purpose of the investigation are met and the correct authorisation procedure is followed before obtaining the data from communication service providers. Advice should be sought from the Legal Services if in doubt.

13.10 Acquisition and disclosure of communications data is also overseen by the Investigatory Powers Commissioner's Office (IPCO).

13.11 The details of the procedure for obtaining communications data can be found at 15.32.

13.12 Under section 11 IPA 2016, it is an offence for a person in a public authority knowingly or recklessly to obtain communications data from a telecommunications operator or postal operator without lawful authority. The Home Office Acquisition and Disclosure of Communications Data Code of Practice can be found on the Home Office website.

14. Use of Social Media/Internet

14.1 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.

14.2 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, as well as compliance with the Data Protection Act 2018 where personal information is likely to be accessed or obtained. Where the RIPA crime threshold is not met, a non RIPA authorisation may still be required. See the non RIPA procedure 6.10.

14.3 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.

14.4 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 if access controls are applied.

14.5 Where privacy settings are available but not applied the data may be considered open source and an authorisation is not usually required. However, in some circumstances where data is considered open source, privacy expectations may still nevertheless apply, and authorisation should be sought. This is because as stated in the Home Office Covert Surveillance and Property Interference Code of Practice the intention of the subject in making the data public was not for it to be used covertly for an investigatory purpose. In deciding whether online surveillance should be regarded as covert, consideration should be given to the likelihood of the subject knowing that surveillance could be taking place.

14.6 If reasonable steps are taken to inform the public or the subjects that surveillance could take place (where appropriate), the surveillance may be deemed as overt, for which authorisation may not be required

14.7 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. An authorisation for the use and conduct of a CHIS is necessary if a relationship is established or maintained by a n officer of the council or by a person acting on the council's behalf (i.e. the activity is more than mere reading of the site's content). This could occur if an officer of the council covertly asks to become a 'friend' of someone on a SNS. It is not unlawful for an officer of the council to set up a false identity, but it is inadvisable for that officer to do so for a covert purpose without an authorisation.

14.8 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". The first visit to an SNS profile which might be displaying lots of private information could be regarded as a 'drive by' however any subsequent 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.

14.9 The following factors should be taken into account when considering using social media sites as part of an investigation:

- whether the investigation/research is directed towards an individual or organisation
- whether it is likely to result in obtaining private information about a person or group of people
- whether it is likely to involve visiting other internet sites to build up an intelligence picture or profile
- whether the information obtained will be recorded or retained and consideration of the appropriate safeguards
- whether the information is likely to provide an observer with a platform of lifestyle
- whether the information is being combined with other sources of information which amounts to information relating to a person's private life
- whether the investigation or research is part of an ongoing piece of work involving repeated viewing of the subject
- whether it is likely to involve identifying and recording information about third parties, such as family or friends of the subject, that may include private information and therefore risk collateral intrusion into the privacy of others.

15. Authorisation Procedures

15.1 AOs for directed surveillance and CHIS AOs are responsible for assessing and authorising covert directed surveillance and the use of a CHIS.

It is the responsibility of AOs to ensure that when applying for judicial authorisation the principles of necessity and proportionality are adequately considered and evidenced; and that reviews and cancellations of authorisations are carried out as required under this Policy.

15.2 Schedule 1 of the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order (2010) prescribes the rank or position of AOs 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 legislation but in Walsall Council it has been determined that it would normally equate to second or third tier management. SRO designates which officers can be AOs. Only these officers can authorise directed surveillance and the use of CHIS. A list of AOs is available at Appendix 1. Any requests for amendments to the lists must be made in writing and sent to the SRO.

15.3 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.

15.4 Authorisation of RIPA Covert Directed Surveillance and Use of a CHIS.

15.5 RIPA activity applies to covert directed surveillance and use of CHIS whether by Council employees or external agencies engaged by the Council. Council officers wishing to undertake directed surveillance or use of a CHIS must complete the relevant application form (see para 15.40) and forward it to the relevant AO.

15.6 RIPA Directed Surveillance and use of a CHIS can only be authorised if the AO 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 6.7 above; and
(c) 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.

15.7 Applicant officers 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

15.8 AOs 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.

15.9 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 AO, particularly when considering the proportionality of the surveillance.

15.10 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 the SRO or Legal Services for advice.

15.11 The activity must be authorised before it takes place. At the time of authorisation, the AO must set a date for review of the authorisation and review it on that date. A copy of the completed Home Office application and authorisation form must be forwarded to the SRO within one week of the authorisation 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.

15.12 **Approval by Magistrates Court**

15.13 Following changes under the Protection of Freedoms Act 2012, there is an additional stage in the process for RIPA Directed Surveillance and CHIS investigatory activities. 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.

15.14 The magistrate will have to decide whether the council's application to grant or renew an authorisation to use RIPA should be approved and it will not come into effect unless and until it is approved by the Magistrates Court.

15.15 A separate application should be completed when the Council is requesting judicial approval for the use of more than one of the RIPA surveillance techniques (i.e. Directed Surveillance and CHIS) at the same time.

15.16 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, Council officers should satisfy themselves that authorisation has been obtained, and what activity has been authorised.

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

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

15.19 **The Role of the Magistrates Court**

15.20 The role of the Magistrates Court is set out in section 32A RIPA (for directed surveillance and CHIS). These sections provide that the authorisation, shall not take effect until the Magistrates Court has made an order approving such authorisation or notice. 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 AO.
- 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:
  - 29(7)(a) (for CHIS),
  - 30(3) (for directed surveillance and CHIS)

15.21 The procedure for applying for directed surveillance or use of a CHIS is:

- Applicant officer obtains preliminary legal advice from the Democratic Services Legal Team

- Applicant officer completes an application
- Authorisation is sought from the AO
- Applicant officer/legal representative creates court pack and applicant officer proceeds to court
- Applicant officer organises the directed surveillance or use of a CHIS to take place
- Applicant officer sends copy Magistrates Court order to the SRO

15.22 **Additional Requirements for Authorisation of a CHIS**

15.23 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 security and welfare of the CHIS
- 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

15.24 A record of decision for CHIS must be completed which covers the requirements that should be in place for handling a CHIS including juvenile and vulnerable CHIS.

15.25 **Requirements for Authorisation of Acquisition and Disclosure of Communications Data**

The rules on the granting of authorisations for the acquisition of communications data are different from directed surveillance and CHIS authorisations and involve three roles within the council.

The roles are:
- Applicant Officer
- Approved Rank Officer
- Senior Responsible Officer

The two external roles are:

- Single Point of Contact (SPoC) at the National Anti-Fraud Network (NAFN)
- AO in the Office of Communications Data Authorisations (OCDA)

15.26 **Applicant and their responsibilities**

The applicant is a person involved in conducting or assisting an investigation or operation and who makes an application in writing or electronically to obtain communications data. Applicants must submit applications through the central NAFN (SPoC) portal. Applicants will need to be registered with NAFN to access the portal and have valid login and security details. An allocated SPoC officer will then check all applications for legal compliance and, where necessary, provide feedback before submitting for authorisation to OCDA. The applicant will complete an application form setting out for consideration the necessity and proportionality of a specific requirement for acquiring communications data.

15.27 Any member of staff engaged in a relevant role i.e. one which requires carrying out investigations may be an applicant, subject to any internal controls or restrictions put in place within public authorities.

The applicant must:

- describe the communications data required, specifying, where relevant, any historic or future date(s) and, where appropriate, time period(s)
- specify the purpose for which the data is required, by reference to a statutory purpose under the Act
- include a unique reference number
- include the name and the office, rank or position held by the person making the application
- describe whether the communications data relates to a victim, a witness, a complainant, a suspect, next of kin, vulnerable person or other person relevant to the investigation or operation
- include the operation name (if applicable) to which the application relates
- identify and explain the time scale within which the data is required
- explain why the acquisition of that data is considered necessary and proportionate to what is sought to be achieved by acquiring it
- present the case for the authorisation in a fair and balanced way. In particular, all reasonable efforts should be made to take account of information which supports or weakens the case for the authorisation
- consider and, where appropriate, describe any meaningful collateral intrusion – the extent to which the rights of any individual not under investigation may be infringed and why that intrusion is justified in the circumstances
- consider and, where appropriate, describe any possible unintended consequences of the application; and
- where data is being sought from a telecommunications operator or postal operator, specify whether the telecommunications operator or postal operator may inform the subject(s) of the fact that an application has been made for their data.

15.28 The applicant should record subsequently whether the application was authorised by an authorising individual and when that decision was made. Applications should be retained by the public authority and be accessible to the SPoC.

15.29 **Approved Rank Officer (ARO)**

This is the Walsall Council officer who is aware that the application is being made by the applicant and is able to verify to the SPoC at NAFN that the acquisition of communications data is necessary and proportionate for the purpose it is required for before it is authorised externally by OCDA. The ARO does not authorise or approve any element of the application and is not required to be operationally independent.

15.30 **Senior Responsible Officer (SRO) and their responsibilities**

The Senior Responsible Officer (SRO) within Walsall Council is the Executive Director Economy and Environment.

15.31 The SRO is responsible for:

- The integrity of the process in place within the public authority to obtain communications data
- engagement with AOs in the Office for Communications
- Data Authorisations (where relevant)
- compliance with Part 3 of the Act and with the Code of Practice, including responsibility for novel or contentious cases
- oversight of the reporting of errors to the IPC and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors
- ensuring the overall quality of applications submitted to OCDA
- engagement with the IPC's inspectors during inspections; and
- where necessary, oversight of the implementation of post-inspection action plans approved by the IPC

Single point of contact (SPoC) and their responsibilities

15.32 The SPoC is an individual trained to facilitate the lawful obtaining of communications data and effective co-operation between a public authority, the Office for Communications Data Authorisations (OCDA) and telecommunications and postal operators. To become accredited an individual must complete a course of training appropriate for the role of a SPoC and have been issued the relevant SPoC unique identifier.

15.33 Public authorities are expected to provide SPoC coverage for all reasonably expected instances of obtaining communications data. Walsall Council is a member of the National Anti-Fraud Network (NAFN). NAFN is an accredited body for the purpose of providing data and intelligence under the IPA for all public bodies. As part of their portfolio, they offer a comprehensive SPoC service.

15.34 The SPoC will:

- assess whether the acquisition of specific communications data from a telecommunications operator or postal operator is reasonably practicable or whether the specific data required is inextricably linked to other data

- advise applicants on the most appropriate methodology for acquisition of data where the data sought engages a number of telecommunications operators or postal operators
- engage with applicants to develop and implement effective strategies to obtain communications data in support of operations or investigations
- advise on and manage the use of the request filter, specifically in relation to progress of requests through the filter and compliance by the filter with the relevant authorisation
- advise on the interpretation of the Act, particularly whether an authorisation is appropriate
- provide assurance that authorisations are lawful under the Act and free from errors
- consider and, where appropriate, provide advice on possible unintended consequences of the application
- assess any cost and resource implications to both the public authority and the telecommunications operator or postal operator of communications data requirements

15.35 SPoC's have received training specifically to facilitate lawful acquisition of communications data and effective co-operation between the council, OCDA and the communication service providers.

15.36 AO at Office of Communications Data Authorisations (OCDA). Communications Data applications no longer require judicial approval as is required for directed surveillance under RIPA. The AO at OCDA scrutinises the application independently and either approves or rejects the application setting out the justification for the decision, taking into account the lawfulness of the conduct, and that the appropriate standards and safeguards have been addressed. The council is not permitted to contact OCDA directly, all correspondence must be through the SPoC at NAFN.

15.37 **The procedure for applying for acquisition of communications data** is as follows:

- Applicant obtains preliminary legal advice from Legal Services.
- Applicant officer creates an application using the Cycomms Web Viewer on the NAFN website.
- SPoC Officer at NAFN triages and accepts the application into the Cyclops system.
- SPoC Officer uses Cyclops to update the application details and completes the SPoC report. As part of this, SPoC checks that the Council is lawfully permitted to obtain Communications Data for the purpose it is required for, determines the conduct such as the type of data needed to achieve the Council's purpose. Where the application is for Events Data, that the legal threshold is met and, in all cases, the conduct is justified based on the seriousness of the offence, the risk of unintended results, the risk of excessive data being obtained, including collateral intrusion, including whether other considerations or recommendations are required.
- The SPoC liaises with applicant officer and Approved Rank Officer if further work is required.

- SPoC sends the application to the Office of Communications Data (OCDA) for external approval on behalf of the council.
- If SPoC receives authorisation from OCDA, SPoC sends request to Communications Service Provider (CSP).
- SPoC receives results back from CSP and returns results to Applicant.
- Applicant accesses the Web Viewer and downloads results.
- Applicant sends details of the investigation, type of data required, whether the application was approved by OCDA and the date for this to the Democratic Services Legal Team who will update the Central Record. If the application is refused by OCDA, the council can either:
  - decide not to proceed with the application
  - resubmit the application with revisions including the justifications for doing so
  - challenge the decision made by OCDA if this is agreed by the SRO
  - further guidance from OCDA can be provided

Completing a Communication Data application form

15.38 An application to acquire communications data must:

- state the type of data required e.g. entity or events data; describe the communications data required e.g. the subscriber details linked to a telephone number, email address etc
- the timescales or specific date or period of the data that it is required. If the data will or may be generated in the future, the future period is restricted to no more than one month from the date on which the authorisation is granted
- specify the purpose for which the data is required and set out the legislation under which the operation or investigation is being conducted. This must be a statutory function of the Council for the prevention or detection of crime or preventing disorder (or for events data, this must meet the threshold for serious crime)
- include a unique reference number
- include the name and the office, rank or position held by the person making and verifying the application
- describe whether the communications data relates to a victim, a witness, a complainant, a suspect, next of kin, vulnerable person or other person relevant to the investigation or operation
- include the operation name (if applicable) to which the application relates
- explain why the acquisition of that data is considered necessary and proportionate in the circumstances based on the link between the investigation, the subject or other individuals and, and why the specific communication data is required, what other lawful, reasonable or least intrusive methods were considered and why these were rejected
- present the case for the authorisation in a fair and balanced way taking into account the size and scope of the investigation. In particular, all reasonable efforts should be made to take account of information which supports or weakens the case for the authorisation
- consider and, where appropriate, describe any risk of meaningful collateral intrusion. the extent to which the privacy rights of any individual not under

investigation may be infringed and why that intrusion is justified in the circumstances. For example, where access is for 'outgoing calls' from a 'home 23 telephone' collateral intrusion may be applicable to calls made by family members who are outside the scope of the investigation. The applicant therefore needs to consider what the impact is on third parties and try to minimise it

- consider and, where appropriate, describe any possible unintended consequences of the application; and
- where data is being sought from a telecommunications operator or postal operator, specify whether the telecommunications operator or postal operator may inform the subject/individual(s) of the fact that an application has been made for their data

Urgent Authorisations

15.39 By virtue of the fact that an authorisation under RIPA is not approved until signed off by a Magistrates Court, urgent oral authorisations are no longer available. Urgent oral authorisations are also not available for Communications Data.

Application Forms

15.40 Only the RIPA Forms listed below can be used by officers applying for RIPA authorisation. The forms should be taken from the Home Office web pages so they are up to date. https://www.gov.uk/government/collections/ripa-forms--2

(a) Directed Surveillance

- Application for Authority for Directed Surveillance
- Review of Directed Surveillance Authority
- Renewal of Directed Surveillance Authority
- Cancellation of Directed Surveillance

(b) CHIS

- Application for Authority for Conduct and Use of a CHIS
- Review of Conduct and Use of a CHIS
- Cancellation of Conduct and Use of a CHIS
- Renewal of Conduct and Use of a CHIS

15.41 Authorisation/notice durations are:

- for covert directed surveillance the authorisation remains valid for 3 months after the date of authorisation
- for a CHIS the authorisation remains valid for 12 months after the date of authorisation (or 4 months if a juvenile CHIS is used)
- a communications data notice remains valid for a maximum of 1 month. All authorisations and notices are expected to specify dates and times for the acquisition or disclosure of the information

Authorisations should not be permitted to expire; they must be either renewed or cancelled when the activity authorised has been completed or is no longer necessary 24 or proportionate in achieving the aim for which it was originally authorised. This is a statutory requirement which means that all authorisations must be reviewed to decide whether to cancel or renew them.

Review of Authorisations

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

15.43 Officers carrying out RIPA/IPA activity, or external agencies engaged by the Council to carry out RIPA/IPA activity, must periodically review it and report back to the AO/Approved Rank Officer if there is any doubt as to whether it should continue. For Juvenile CHIS, the relevant Code of Practice stipulates that the authorisation should be reviewed on a monthly basis.

15.44 All reviews should be recorded on the appropriate Home Office form.

15.45 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 updated.

Renewal of Authorisations

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

15.47 Renewed authorisations will normally be for a period of up to 3 months for covert directed surveillance, 12 months in the case of CHIS, 4 months in the case of juvenile CHIS and 1 month in the case of a communications data authorisation. Authorisations may be renewed more than once, provided they are considered again and continue to meet the criteria for authorisation.

15.48 Applications for the renewal of an authorisation for covert directed surveillance or CHIS authorisation must be made on the appropriate form and added as an addendum to the application form which granted the initial authorisation.

15.49 All RIPA renewals will require an order of the Magistrates Court.

15.50 A copy of the council's notice of renewal of an authorisation must be sent to the SRO within one week of the renewal together with a copy of the Magistrates Court order renewing the authorisation to enable the central record on RIPA to be updated.

15.51 For communications data, renewals must be made via the NAFN SPoC and authorised by OCDA. The reasoning for seeking renewal of a communications data authorisation should be set out by the applicant in an addendum to the application form which granted the initial authorisation.

Cancellation of Authorisations

15.52 The person who applied for or last renewed the authorisation must cancel it when they are satisfied that the covert directed surveillance, CHIS or communications data authorisation or notice no longer meets the criteria for authorisation such as when it is no longer necessary for the statutory purpose, or the activity is no longer deemed to be proportionate. For covert directed surveillance and CHIS cancellations must be made on the appropriate Home Office form (see paragraph 15.40).

15.53 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 addressed.

15.54 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.

15.55 For Communications Data, the NAFN SPoC must be made aware of the cancellation who will cease the authorised activity, ensure any notices are cancelled and inform the Communication Service Provider.

15.56 What happens if the surveillance has unexpected results?

15.57 Those carrying out the covert surveillance should inform the AO 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.

15.58 Errors

15.59 Proper application of the RIPA provisions, and robust technical systems, should reduce the scope for making errors. A senior officer within a public authority is required to undertake a regular review of errors and a written record must be made of each review. For the council, this will be the SRO.

15.60 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.

15.61 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 Code of Practice. 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 the IPCO is set out in the relevant Home Office Codes of Practice

16 Records and Documentation

16.1 Departmental Records Applications, renewals, cancellations, reviews and copies of notices must be retained by the council in written or electronic form, and physically attached or cross referenced where they are associated with each other. These records will be confidential and should be retained for a period of at least five years from the ending of the authorisation and destroyed in accordance with the council's Retention and Disposal Policy. Where it is believed that the records could be relevant to pending or future court proceedings, they should be retained and then destroyed five years after last use.

16.2 In relation to communications data, records must also be held centrally by the SPoC. These records must be available for inspection by the IPCO and retained to allow the Investigatory Powers Tribunal to carry out its functions.

16.3 A central record central record of authorisations, renewals, reviews and cancellations is maintained by:

Executive Director Economy, Environment and Communities
Walsall Council
Darwall Street
Walsall
WS1 1TP

16.5 The central record is maintained in accordance with the requirements set out in the Home Office Codes of Practice. In order to keep the central record up to date AOs/applicant officers must, in addition to sending through the Home Office application, authorisation form, Magistrates Court order or OCDA decision documents within one week of the authorisation being approved by the Magistrates Court or OCDA, send notification (by e-mail) of every renewal, cancellation and review on the council's notification forms (see paragraphs 15.40).

17. Safeguarding and the Use of Material.

17.1 All material obtained through the use of directed surveillance, CHIS or acquisition of communications data records containing personal data must be handled in accordance with the Data Protection Act 2018 (DPA) and the Council's Data Protection Policy.

17.2 The data protection principles under the DPA includes that personal data should only be processed if it is lawful to do so, that the data are adequate, relevant and not excessive for the purpose it was collected.

17.3 A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data Care must also be taken that personal data collected as part of an investigation is held in a manner that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. A personal data breach may need to be reported to the Information Commissioner's Office within 72 hours of officers becoming aware of the breach.

17.4 To mitigate against risk of personal data being compromised, all records and materials should be stored securely; clearly labelled; classified where appropriate as OFFICIAL or SENSITIVE to demonstrate the degree of sensitivity of the information; the appropriate retention period should be recorded at the outset and reviewed. Access to material obtained should be limited to those officers that have a legitimate reason for storing or accessing the records, with appropriate access controls in place. The data should not be stored for any longer than is necessary for any authorised purpose, and thereafter securely destroyed. This applies to all copies, extracts and summaries of the material obtained.

17.5 Where an authorisation results in excessive data having been acquired, the data should only be retained where it's appropriate and lawful to do so. The data must be reviewed to determine whether there is an intention to use it, and the reasons for requiring it, including whether retention of the data is necessary and proportionate contact Legal services if advice is required.

17.6 IPCO has produced recommendations in respect of safeguarding data (6 Data Assurance steps) that the council is required to demonstrate compliance with. The recommendations can be found at **Appendix 4** of this Policy.

17.7 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.

17.8 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.

17.9 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.

17.10 In addition to the data protection considerations above, material obtained must be used, stored and destroyed in compliance with any other legal requirements, including confidentiality. Information Security guidance is available on the intranet at the Protecting Information pages.

18. Use of Material as Evidence

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

19. Disseminating Material

19.1 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.

19.2 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.

19.3 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.

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

20.1 The SRO will arrange regular training on RIPA. All AOs; 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.

20.2 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.

21. Complaints

21.1 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 - List of Authorised Officer posts

Post & Current Post Holder	Scope of Authorisation
Head of Community Safety and Enforcement Current Incumbent David Elrington	Local Authority applications 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.
Director of Resilient Communities Current Incumbent Paul Gordon	Local Authority applications 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.
Director of Governance and Monitoring Officer Current Incumbent Anthony Cox	Local Authority applications 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.
Executive Director Economy & Environment Current Incumbent Dave Brown	Local Authority applications 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.
Chief Executive Current Incumbent Emma Bennett	Applications for covert human intelligence source (CHIS) where the CHIS is a juvenile / vulnerable adult. In her absence, this can be a person acting as the Head of Paid Service.
All Executive Directors	Applications for covert human intelligence source (CHIS) where the CHIS is a juvenile / vulnerable adults only in the absence of the Chief Executive.

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 2 Non RIPA Authorisation

Unique Reference Number

Non-RIPA - Authorisation

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

DETAILS OF APPLICATION
Give rank or position of AO:
AO: **Rank:** **Has a pre-surveillance risk assessment been carried out? Yes No** **Standard Risk Assessment for these exercises**
Describe the purpose of the specific operation or investigation.

The identities, where known, of those to be subject of the surveillance.
Explain the information that it is desired to obtain as a result of the surveillance.
Identify on which grounds the surveillance is <u>necessary.</u>
• For the purpose of preventing or detecting crime or of preventing disorder;
Explain <u>why</u> this surveillance is necessary on the grounds you have identified.
Supply details of any potential collateral intrusion and why the intrusion is unavoidable. Describe precautions you will take to minimise collateral intrusion.
Explain <u>why</u> this 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?
1. Confidential information. INDICATE THE LIKELIHOOD OF ACQUIRING ANY CONFIDENTIAL INFORMATION:

2. Applicant's Details			
Name (print)		**Tel No:**	
Grade/Rank		**Date**	
Signature			

3. AO'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:

Who:

What:

Where:

When

How:

4. Explain <u>why</u> you believe the surveillance is necessary.

5. Explain why you believe the surveillance to be proportionate to what is sought to be achieved by carrying it out.

Date of first review	

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.

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]				

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 December 2022 CHIS Code (publishing.service.gov.uk)

Appendix 4 IPCO 6 Data Assurance steps

The Investigatory Powers Commissioner's Office recommends that authorities take the following actions to help assist with demonstrating compliance and adherence to obligations regarding the safeguard any data that has already been obtained or that may be obtained under RIPA or IPA:

1) Review the safeguarding obligations in the relevant Home Office Code of Practice for directed surveillance, CHIS, and Communications Data.

2) Ensure that internal safeguarding policies for retaining, reviewing and disposing of any relevant data are accurate and up to date.

3) Ensure that the AO/approved rank officer has a full understanding of any data pathways used for RIPA/IPA, such as where the data is stored, who has access and why, how the data is protected from unauthorised access.

4) Ensure that all data obtained under IPA and RIPA is clearly labelled and stored securely with a known retention policy.

5) Review the wording of safeguards in any applications to obtain data under IPA and RIPA and ensure that they accurately reflect the internal retention and disposal processes.

6) Review whether data obtained under previous authorisations is being retained for longer than is necessary and, if appropriate, consider disposing of retained data. If the data is still required, it must be lawful, necessary and proportionate.