Appendix 2: Corporate Operating Procedure

CITY OF WOLVERHAMPTON COUNCIL

Regulation of Investigatory Powers Act 2000
Investigatory Powers Act 2016
Corporate Operating Procedure

1.0 Background

1.1 Officers undertaking activities covered by this Operating Procedure shall have regard to the following: RIPA Home Office Codes of Practice, the Procedures and Guidance documents produced by the Office of Surveillance Commissioners Office and subsequently by the Investigatory Powers Commissioners Office, the Data Protection Act 2018, the Police and Criminal Evidence Act 1984 and the Criminal Procedure and Investigation Act 1996 and Codes of Practice issued thereunder.

2.0 Legal implications of RIPA 2000

2.1 This Operating Procedure details the operational delivery of RIPA 2000 and IPA 2016 activities by City of Wolverhampton Council officers and supports the Covert Investigations Policy. Activities carried out in accordance with this Operating Procedure are assumed to be in compliance with the Human Rights Act 1998.

2.2 Authorising Officers

Authorising Officers for RIPA controlled activities are listed in Appendix 1 of the Councils Covert Investigations Policy.

Where authorisation is likely to obtain confidential information, it MUST be authorised by the Chief Executive as Head of Paid Service.

2.3 Definitions

2.3.1 Communications Data

- The term ‘communications data’ includes the ‘who’, ‘when’, ‘where’, and ‘how’ of a communication but not the content i.e. what was said or written.

- It includes the way in which, and by what method, a person or thing communicates with another person or thing. It excludes anything within a communication including text, audio and video that reveals the meaning, other than inferred meaning, of the communication.

- It can include the address to which a letter is sent, the time and duration of a communication, the telephone number or email address of the originator and recipient, and the location of the device from which the communication was made. It covers electronic communications including internet access, internet telephony, instant messaging and the use of applications. It also includes postal services.

- Communications data is generated, held or obtained in the provision, delivery and maintenance of communications services – i.e. postal services or telecommunications services.

All communications data held by a telecommunications operator or obtainable from a telecommunication system falls into two categories:

- entity data – this data is about entities or links between them and describes or identifies the entity but does not include information about individual events. Entities could be individuals, groups and objects (such as mobile phones or other communications devices);
- events data – events data identifies or describes events in relation to a telecommunication system which consist of one or more entities engaging in an activity at a specific point, or points, in time.

The authorisation levels required to access communications data reflect the fact that the set of events data as a whole contains the more intrusive communications data, including information on who has been in communication with whom, a person's location when their mobile device connects to the network and internet connection records.

2.3.2 Covert Surveillance

Surveillance for the purposes of RIPA includes monitoring, observing or listening to persons their movements, conversations or other activities and communications. It may be conducted with or without the assistance of a surveillance device and includes the recording of any information obtained.

Surveillance is covert if, and only if, it is carried out in a manner calculated to ensure that any persons who are subject to the surveillance are unaware that it is or may be taking place. There are two types of covert surveillance:

- **Intrusive surveillance** is covert surveillance that is carried out in relation to anything taking place on residential premises or in any private vehicle (and that involves the presence of an individual on the premises or in the vehicle) or is carried out by a means of a surveillance device. The definition of surveillance as intrusive relates to the location of the surveillance, and not any other consideration of the nature of the information that is expected to be obtained.

  Intrusive Surveillance is NOT available to Local Authorities.

- **Directed surveillance** is covert surveillance that is not intrusive but is carried out in relation to a specific investigation or operation in such a manner as is likely to result in the obtaining of private information about any person (other than by way of an immediate response to events or circumstances, such that it is not reasonably practicable to seek authorisation under RIPA).

2.3.3 Covert Human Intelligence Source

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 paragraph 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.

2.3.4 Confidential Material

Confidential personal information (such as medical records or spiritual counselling), confidential journalistic material, confidential discussions between Members of Parliament and their constituents, or matters subject to legal privilege (which includes certain communications between professional legal advisers and their clients or persons representing the client)

2.4 Authorisation Criteria

Authorising Officers shall be aware of and have regard to the Covert Investigations Policy in carrying out their duties. Officers requesting authorisation **must** satisfy the Authorising Officer that the action is **proportionate** to the nature of the matter under investigation and is **necessary**, they must provide sufficient justification/intelligence to support the application.

2.4.1 **Necessity**: The person granting an authorisation must believe that the activities to be authorised are **necessary** on one or more statutory ground. The only ground available to a Local Authority officer when authorising Directed Surveillance, a Covert Human Intelligence Source or access to Communications Data is:

For the prevention or detection of crime

Authorising Officers **shall** satisfy themselves that the activities proposed are **necessary and proportionate** before issuing an authorisation and **must**

explain the reasons for their belief in the Authorising Officers Comments section of the relevant authorisation form. A legal empowerment to act **does not** mean the action will be proportionate. A balance between the level of intrusion and the public interest must be **manifestly** demonstrated and support the activity's necessity.

An Authorising Officer may only grant an authorisation for the carrying out of Directed Surveillance for the purpose of preventing or detecting a criminal offence if it meets additional conditions, namely that the offence under investigation is punishable on summary or indictment by a maximum term of at least 6 months of imprisonment or would constitute an offence under S146, S147 and S147A of the Licensing Act 2003 (namely the sale of alcohol to children, allowing the sale of alcohol to children and persistently selling alcohol to children) or S7 of the Children and Young Persons Act 1933 (sale of tobacco, etc to persons under 18).

2.4.2 **Proportionality**: Involves balancing the seriousness of the intrusion into the privacy of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative and operational terms.

The authorisation will not be proportionate if it is excessive in the overall circumstances of the case. The following elements of **proportionality** should therefore be considered:

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

2.5 Approval by Magistrates Courts

2.5.1 Sections 37 and 38 of the Protection of Freedoms Act 2012 require a local authority who wish to authorise the use of Directed Surveillance and use of a CHIS under RIPA to obtain an order approving the grant or renewal of an authorisation or notice from a JP (a District Judge or lay magistrate) before it can take effect. If the JP is satisfied that the statutory tests have been met and that the use of the technique is necessary and proportionate he/she will issue an order approving the grant or renewal for the use of the technique as described in the application.

2.5.2 Officers shall have regard to the Home Office Guidance to Local Authorities in England and Wales on the judicial approval process for RIPA and the crime threshold for Directed Surveillance.

3.0 Compliance Systems for RIPA 2000

3.1 Communications Data

Officers shall have regard to the Home Office Communications Data Code of Practice (November 2018).

3.1.1 Access to Communications Data

An applicant must complete the relevant Application for Communications Data form which is available on the NAFN portal. This **must be** submitted to NAFN and the Applicant must notify the designated 'approved rank officer', identified in Appendix 1 of the Corporate Policy, that the application is being made. The local authority senior responsible officer must be satisfied that the officer(s) verifying the application are of an appropriate rank and must inform NAFN of such nominations.

NAFN will be responsible for submitting the application to OCDA on behalf of the local authority.

A local authority may not make an application that requires the processing or disclosure of internet connection records for any purpose.

Under section 11 of the Investigatory Powers Act 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.

3.1.2 Recording telephone conversations

The recording or monitoring of one or both ends of a telephone conversation by a surveillance device as part of an authorised directed surveillance operation will not constitute interception under Part 2 or Chapter 1 of Part 6 of the 2016 Act provided the process by which the product is obtained does not involve any modification of, or interference with, the telecommunication system or its operation and the surveillance is not intrusive as this is not available to a local authority.

3.1.3 Errors

There may be rare occasions when communications data is wrongly acquired or disclosed. In these cases, the public authority which made the error, or established that the error had been made, must report the error to the

authority's senior responsible officer and the IPC. In accordance with section 231 of the Act, when an error is reported to the IPC, the IPC may inform the affected individual, who may make a complaint to the IPT.

3.2 Directed Surveillance

Officers shall have regard to the Home Office Covert Surveillance and Property Interference Revised Code of Practice (August 2018) and guidance produced by the Investigatory Powers Commissioners Office, plus the City of Wolverhampton Councils Social Media in Investigations Policy.

3.2.1 Directed Surveillance undertaken

- for the purposes of a specific investigation or operation

- in such a manner as is likely to result in the obtaining of private information (includes private business information) about any person whether or not an identified target and

- otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be practicable for an authorisation to be sought

WILL be deemed to be covert and require authorisation

The Investigating officer must obtain an Investigation Reference number for the application from their Service Lead/Manager and the applicant must obtain a Unique Reference Number from the RIPA Co-ordinator prior to each application being made.

Applicants must then complete and submit an Authorisation of Directed Surveillance form **[WCCRIPA 2000(3)]** to the Authorising Officer, providing sufficient detail to justify necessity and proportionality of the activities, unless:

- notification of surveillance for a **specified period** has been given to the target
- surveillance of activities is undertaken as part of an announced visit to the premises or is **clearly overt**.
- surveillance is of limited duration undertaken as a first response to a complaint or on an officer's own initiative and hence is not directed or is a response to arising events

NB The 'directing' of CCTV equipment to monitor a particular target location to address a known pattern of offending **must be authorised**.

3.2.2 Directed surveillance **must be authorised against a specific offence** which meets the criminal threshold (see 3.2.3 below), and the type and the timing of the deployment of the surveillance will always reflect this.

3.2.3 Local authorities can only authorise use of Directed Surveillance under RIPA to prevent or detect criminal offences that are either punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months' imprisonment **or** are related to the underage sale of alcohol and tobacco. The offences relating to the latter are in article 7A of the 2010 Order.

3.2.4 Local authorities **cannot** authorise Directed Surveillance for the purpose of preventing disorder unless this involves a criminal offence(s) punishable (whether on summary conviction or indictment) by a maximum term of at least 6 months' imprisonment.

3.2.5 Local authorities may therefore continue to authorise use of Directed Surveillance in more serious cases as long as the other tests are met – i.e. that it is necessary and proportionate and where prior approval from a JP has been granted. Examples of cases where the offence being investigated attracts a maximum custodial sentence of six months or more could include more serious criminal damage, dangerous waste dumping and serious or serial benefit fraud.

3.2.6 Local authorities may also continue to authorise the use of Directed Surveillance for the purpose of preventing or detecting specified criminal offences relating to the underage sale of alcohol and tobacco where the necessity and proportionality test is met and prior approval from a JP has been granted.

3.2.7 A local authority **may not authorise** the use of Directed Surveillance under RIPA to investigate disorder that does not involve criminal offences or to investigate low-level offences where the maximum term of imprisonment is less than six months.

3.2.8 Once an Authorisation of Directed Surveillance form **[WCCRIPA 2000(3)]** has been completed and authorised, the Authorising Officer will need to obtain an order approving the grant of the authorisation from a JP (a District Judge or lay magistrate) before it can take effect. If the JP is satisfied that the statutory tests have been met and that the use of the technique is necessary and proportionate he/she will issue an order approving the grant for the use of the technique as described in the application form. An application for Judicial Approval Form **[WCCRIPA 2000(MCA)]** should be completed before a hearing is arranged with the court. All supporting documentation as detailed on the form must be taken to court.

When there is knowledge that **Confidential Material** is likely to be acquired then Authorisation **must** be sought from the Head of Paid Service (Chief Executive). Confidential Material includes material subject to legal privilege, material disclosing details of physical or mental health or spiritual counselling or material held in confidence for journalistic purposes.

3.2.9 The crime threshold applies only to the authorisation of **Directed Surveillance** by local authorities under RIPA, not to the authorisation of local

authority use of CHIS or their acquisition of Communications Data. The threshold came into effect on 1 November 2012.

3.2.10 The statutory RIPA Code of Practice on Covert Surveillance and Property Interference makes it clear that routine patrols, observation at trouble 'hotspots', immediate response to events and overt use of CCTV are all techniques which do not require RIPA authorisation.

3.3 Covert Human Intelligence Sources (CHIS)

Officers shall have regard to the Home Office Covert Human Intelligence Sources Revised Code of Practice (August 2018) and the OSC Procedures and Guidance (July 2016).

3.3.1 The use of Council Officers or third parties to obtain information from the subject of an investigation in a covert manner by the establishment or maintenance of a relationship with the subject and activities where a **significant** degree of 'relationship' arises may constitute use as a CHIS eg:

- Test purchasing of goods by officers
- Traders or consumers continued involvement in transactions relating to the supply of illegal goods to permit investigation of their production, importation or distribution

The following criteria **tend** to indicate that the activities require authorisation

- Arranged meetings to facilitate purchase e.g. by contact solicited by advertisement
- Visit to domestic or non-retail premises to facilitate purchase
- Degree of discussion surrounding purchase activity, particularly where officers utilise `cover' stories as part of the discussion

3.3.2 An Authorisation of the Use or Conduct of a Covert Human Intelligence Source form **[WCCRIPA 2000(7)]** shall be completed and submitted to an authorising officer for consideration.
The Investigating officer must obtain an Investigation Reference number for the application from their Service Lead/Manager and the applicant must obtain a Unique Reference Number from the RIPA Co-ordinator prior to each application being made.

3.3.3 A '**Controller' shall** be identified for the CHIS
The role of controller will be undertaken by a 'covert operations manager' who shall be at least the level of Service Lead/Manager.
The 'controller' will be responsible for the management and supervision of the 'handler' and general oversight of the use of the CHIS including the proper assessment of any health & safety risks.

3.3.4 A **'Handler' shall** be identified for the CHIS
The role of the handler will be undertaken by a person referred to as a 'cover officer', the handler will have day-to-day responsibility for:

- dealing with the CHIS on behalf of the authority concerned
- directing the day-to-day activities of the CHIS
- recording the information supplied by the CHIS; and
- monitoring the CHIS's security and welfare.

3.3.5 **Juvenile CHIS**: Officers authorising a Juvenile CHIS **(Under 18)** shall ensure that there is no conflict of interest between the source and any relatives of the source and the target. Juveniles used to test purchase goods subject to age related sale controls shall be recruited in accordance with the BRDO Age Restricted Products and Services: A Code of Practice for Regulatory Delivery

In addition, OSC Procedures and Guidance (July 2016) [para 244] gives guidance in relation to test purchase of sales to juveniles.
'*When a young person pursuant to an arrangement with an officer of a public authority, carries out a test purchase at a shop, he is unlikely to be construed as a CHIS on a single transaction, but this would change if the juvenile revisits the same establishment in a way that encourages familiarity. If covert recording equipment is worn by the test purchaser, or an adult is observing the test purchase, it will be desirable to obtain an authorisation for directed surveillance because the ECHR has construed the manner in which a business is run as private information and such authorisation must identify the premises involved. In all cases a prior risk assessment is essential in relation to a young person*'.

3.3.6 The authorisation for the use of a CHIS likely to obtain confidential information or the deployment of a juvenile or vulnerable person (by virtue of mental or other condition) as a CHIS requires authorisation by the most senior local authority officer – Head of Paid Service (Chief Executive) or, in his absence, the acting Head of Paid Service.

3.3.7 The Authorising Officer will need to obtain an order approving the grant of the authorisation from a JP (a District Judge or lay magistrate) before it can take effect. If the JP is satisfied that the statutory tests have been met and that the use of the technique is necessary and proportionate he/she will issue an order approving the grant for the use of the technique as described in the application. An application for Judicial Approval Form **[WCCRIPA 2000(MCA)]** should be completed and a hearing arranged with the court where all supporting documentation will be required.

3.3.8 Where the authority has utilised a CHIS, officers must have regard to the Source Records Regulations SI 2000/2725. Detailed records must be kept of the authorisation and use made of a CHIS.

3.3.9 Section 29(5) of the 2000 Act provides that an authorising officer must not grant an authorisation for the use or conduct of a CHIS unless they believe that there are arrangements in place for ensuring that there is at all times a person with the responsibility for maintaining a record of the use made of the

CHIS. The Regulation of Investigatory Powers (Source Records) Regulations 2000; SI No: 2725 detail the particulars that must be included in these records.

3.4 Time Limits

3.4.1 All authorisations **must be issued for the Statutory Time Limits** namely three months for directed surveillance authorisations and twelve months for a Covert Human Intelligence Source, or four months if the CHIS is 18 or less. These will take effect from the date the JP has approved the grant.

Applications for Communications Data will be processed by NAFN SPoC's who will provide all the necessary advice and guidance in relation to time limits to be applied.

3.5 Review of Authorisations

3.5.1 All authorisations shall have review frequencies set by the Authorising Officer on authorisation. Authorising Officers shall ensure review frequencies are met and that the Review of Authorisation form **[WCCRIPA 2000(4)]** for Directed Surveillance or **[WCCRIPA 2000(8)]** for CHIS are completed and authorised in a timely manner.
Officers authorised to undertake activities shall report any change of circumstances affecting the authorisation to the Authorising Officer as soon as possible.

3.6 Renewal of Authorisations

3.6.1 Authorising Officers shall assess the outcomes of the previously authorised activity and shall only grant renewal of an authorisation where it continues to be necessary and proportionate. A Renewal of Authorisation form **[WCCRIPA 2000(5)]** for Directed Surveillance or **[WCCRIPA 2000(9)]** for CHIS shall be completed and authorised. Where investigating officers seek renewal of authorisations the full authorisation file shall be presented to the Authorising Officer. Officers authorised to undertake activities shall report any change of circumstances affecting the authorisation to the Authorising Officer as soon as possible.

3.6.2 The Authorising Officer will need to obtain an order approving the grant of the authorisation from a JP (a District Judge or lay magistrate) before it can take effect. If the JP is satisfied that the statutory tests have been met and that the use of the technique is necessary and proportionate he/she will issue an order approving the renewal for the use of the technique as described in the application. A further application for Judicial Approval Form **[WCCRIPA 2000(MCA)]** should be completed and a hearing arranged with the court where all supporting documentation will be required.

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

3.6.4 Applications for renewals should not be made until shortly before the original authorisation period is due to expire but local authorities must take account of factors which may delay the renewal process (e.g. intervening weekends or the availability of the relevant local authority Authorising Officer and a JP to consider the application).

3.7 Cancellation of Authorisations

3.7.1 Authorising Officers conducting reviews shall consider the continued necessity for the authorisation and cancel it if appropriate. Officers authorised to undertake activities shall report any change of circumstances affecting the authorisation to the Authorising Officer as soon as possible. A Cancellation of Authorisation form **[WCCRIPA 2000(6)]** for Directed Surveillance or **[WCCRIPA 2000(10)]** for CHIS shall be completed and authorised.

3.7.2 All authorised activity must cease when the authorisation is cancelled, the authorisation shall not be cancelled prior to the activity ceasing.

3.8 Errors

Where an error has occurred, or it is established that an error had been made, it must be reported to authority's senior responsible officer immediately. The SRO has oversight of the reporting of errors to the Investigatory Powers Commissioner and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors.

3.9 Urgent Authorisations

Local Authorities are no longer able to orally authorise the use of RIPA techniques, all authorisations must be made in writing and require approval by the Magistrates Court before they take effect.

4.0 Processing Authorisations/Applications under Parts I and II

4.1 Officers **shall** ensure an Investigation Reference Number (Service/Year/Investigation Number e.g. RS/15/01) is allocated to each investigation. These must be obtained from a Service Lead/Manager. An Operation Name is optional.

4.2 Officers shall consider producing an Operation Brief to support the authorisation particularly where:

- there are multiple targets, premises etc

- activities involve teams of officers operating over a considerable period of time
- where the activities authorised are complex.

4.3 Where an operation requires the authorisation of more than one type of activity **all appropriate forms** shall be completed and authorised, referenced by a common Investigation Reference Number.

5.0 Record of Authorised Activities

5.1 Once an Authorisation has been generated and prior to authorisation a Unique Reference Number must be obtained by the Applicant from the RIPA Co-ordinator, who shall promptly record the details on the Central Record of Authorisations.

5.2 Officers shall record full details of all activities carried out under a RIPA authorisation.

5.3 Officers shall avoid as far as possible recording details of activities carried out under an authorisation in different recording mediums. Where this is unavoidable one referencing document shall be maintained.

5.4 Where video or audio recordings are used as part of the surveillance subject to an authorisation a record must be maintained of the media used, when and where it is stored and any distribution of the material during the course of the investigation.

6.0 Maintenance of Authorisation Records

6.1 **All** original Authorisations shall be submitted to the RIPA Co-ordinator in Public Protection, within one week of being signed. These will be filed in a Central Record and be available for inspection by the Commissioners. The filing system is permanently secured.

6.2 Copies of authorisations may be held by Authorising Officers with supporting activity records in a service filing system.

6.3 All copies of Authorisations and activity records (including audio, video recordings, photographs, etc) shall be securely stored when not in use. All records and Authorisations shall be retained in accordance with the requirements of the Criminal Procedure and Investigation Act 1996 or 6 years from the conclusion of the Authorisation whichever is the longer. All media must be retained securely and disposed of in a timely manner with a documented audit trail.

6.4 All media used and information obtained during the course of the authorisation must be retained securely. A record should be made when any material is distributed during the course of the authorisation and subsequent investigation, with an auditable trail of distribution. Retention and disposal dates should be considered at the outset, all media and information should be securely disposed of in a timely manner, with a documented audit trail. Subject to all relevant legislative requirements.

6.5 The RIPA Co-ordinator shall ensure that the Senior Responsible Officer is kept informed of all Authorisations and any quality control issues that are identified.

7.0 Management of Authorisations

7.1 The Senior Responsible Officer shall be responsible for an Audit Plan to ensure all RIPA activities are audited yearly. The RIPA Co-ordinator shall be responsible for organising and delivering the Audit Plan as part of the process of compiling Annual Returns for the Investigatory Powers Commissioners Office. This will provide an Annual Review of the Councils RIPA Authorisation activity.

7.2 Audit results, non-conformances recorded and proposed preventive action shall be agreed with managers responsible for the operational units audited and reported to the Senior Responsible Officer as soon as practicable. Audit records shall be maintained for 5 years.

7.3 The RIPA Co-ordinator shall regularly review RIPA 2000 guidance and disseminate to Authorising Officers and potential applicants.

7.4 The RIPA Co-ordinator will maintain records of training attended.

7.5 The RIPA Co-ordinator shall maintain a controlled documents master list relating to RIPA system documents.

8.0 Referenced Documents

ACPO Good Practice Guide for Computer-Based Evidence
Covert Surveillance and Property Interference Revised Code of Practice (August 2018)
Covert Human Intelligence Sources Revised Code of Practice (August 2018)
Communications Data Code of Practice (November 2018)
OSC Procedures and Guidance (July 2016)
City of Wolverhampton Council Social Media in Investigations Policy
BRDO Age Restricted Products and Services: A Code of Practice for Regulatory Delivery (April 2014)