Appendix 4

Corporate Policy and Procedures on the Regulation of Investigatory Powers Act 2000 (RIPA)

(As amended by the Protection of Freedoms Act 2012)

Walsall Council

Glossary

CCTV	Closed Circuit Television.
CHIS	Covert Human Intelligence Source. A person who establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything that covertly uses such a relationship to obtain information or to provide access to information to another person; or covertly discloses information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship.
CSP	Communications Service Provider. A communications service provider or CSP is a service provider that transports information electronically.
DAT recorder	Digital Audio Tape Recorder. A digital sound recording device.
HRA	Human Rights Act 1998.
NAFN	National Anti Fraud Network. NAFN is a data and intelligence service.
OSC	Office of the Surveillance Commissioner. The OSC's aim is to provide effective and efficient oversight of the conduct of covert surveillance and covert human intelligence sources by public authorities in accordance with law.
RIPA	Regulation of Investigatory Powers Act 2000
SPOC	Single Point of Contact. The means by which communications data is obtained.
SRO	Senior Responsible Officer. Currently this post is designated to the Executive Director – Economy and Environment.

Contents

1	Introduction and key messages
2	Legislative background
3	Surveillance
3.1	Types of surveillance
3.1.2	Overt surveillance
3.1.3	Covert surveillance
3.1.4	Directed surveillance
3.1.5	Intrusive surveillance
3.1.6	Directed surveillance and social media
3.1.7	Covert Human Intelligence Source (CHIS)
3.1.7.1	Juvenile sources
3.1.7.2	Vulnerable individuals
3.1.7.3	Rocords and CHIS
3.2	Authorising officers responsibilities
3.3	Test purchasing
3.4	Anti social behaviour
4	Communications data
5	Confidential information
6	Collateral intrusion
7	Retention and destruction of product of surveillance
8	Monitoring
9	Principles of surveillance
10	Authorisation procedure
10.1	Directed surveillance
10.2	Assessment of the application form
11	Time periods and limitations
12	Oversight and complaints
Appendices	
1	The Magistrates' Approval Process
2	List of Authorised Officer Posts for Authorising Directed Surveillance
3	List of Designated Persons for Granting Authorisations for Accessing Communications Data
4	Flow Chart for Approval of Communications Data Applications
5	Flow Chart for Approval of Covert Human Intelligence Sources (CHIS) Applications

1. Introduction and key messages

1.1 This corporate policy and procedures document is based upon the requirements of the Regulation of Investigatory Powers Act 2000 ('RIPA') and Home Office's Code of Practices on Covert Surveillance and Property Interference 2014; Covert Human Intelligence Sources 2014 and Covert Surveillance and Property Interference 2015. These procedures should be read in conjunction with the Home Office's Codes of Practice. Covert surveillance should be used only in circumstances where it is necessary and proportionate having considered all the requirements of the codes. Copies of the Home Office's Codes of Practice are available on the Home Office website. The website code should be consulted from time to time, and at annual review to ensure this document remains up-to-date. This policy also incorporates the changes brought in by The Protection of Freedoms Act 2012.

1.2 Chapter 2 of Part 2 of the Protection of Freedoms Act 2012 (sections 37 and 38) came into force on 1 November 2012. From then local authorities were required to obtain the approval of a Justice of the Peace (JP) for the use of any one of the three covert investigatory techniques available to them under RIPA namely Directed Surveillance, the deployment of a Covert Human Intelligence Source (CHIS) and accessing communications data. The process to obtain the approval of a Justice of the Peace is attached as Appendix 1. From December 2014, additionally, applications for communications data can only be made via National Anti Fraud Network (NAFN)

1.3 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, Covert Human Intelligence Sources, and Communications Data. This policy and procedure document will therefore be kept under annual review by the Executive Director of Economy & Environment, who is the nominated Senior Responsible Officer (SRO) for the purpose of RIPA. Authorising Officers must bring any suggestions for continuous improvement of this document to the attention of the Executive Director for Economy & Environment at the earliest opportunity. If any of the Home Office Codes of Practice change, or there is a change in legislation, this document will be amended accordingly to reflect those changes.

1.4 At no time should the Council undertake any surveillance if it interferes with any private property. Placing tracking devices on a subject vehicle or person are not authorised for local authorities and must not be used. Again, if anyone is under any doubt on RIPA, this document or the related legislative provisions, they will need to consult with the SRO or the Councils Monitoring Officer, at the earliest opportunity.

1.5 The SRO will check the Register of all RIPA Authorisations, reviews, renewals, cancellations and rejections in accordance with paragraph 8 below (monitoring).

1.6 The objective of this policy and procedure is to ensure that all covert directed surveillance by officers is carried out effectively and is properly authorised in accordance with the law.

1.7 Employee related matters - following a decision of the Investigatory Powers Tribunal, it was established that RIPA authorisation is not required where the surveillance is undertaken as part of an investigation in relation to an employee's misconduct or breach of the terms and conditions of the employee's contract of employment, i.e. any investigation undertaken other than arising from an investigation undertaken in compliance with a statutory function. Another example of an area where non RIPA Surveillance can be undertaken include investigating suspected fraudulent Personal Injury claims.

1.8 This contrasts with authorised surveillance under RIPA that would be undertaken to allow a public authority to comply with its statutory functions, e.g. benefit fraud, or illegal dumping of waste. However, such non RIPA surveillance may still potentially be viewed as infringing the employee's right to privacy as established under Article 8 of the Human Rights Act.

1.9 Where such surveillance, pertaining to a non-criminal investigation into the conduct of an employee, is required, officers are required to complete the appropriate form(s), which can be found on the intranet and then forward them to an authorising officer for approval. For purposes of consistency, authorisations will last for 3 months and appropriate action must be taken to review, renew and cancel authorisations. The authorising officer will apply the same criteria as if the request was for RIPA authorisation, such as considering the necessity and proportionality of the surveillance against the subject of the investigation, the requirement to avoid, wherever possible obtaining confidential information and limiting collateral intrusion still remain. Once authorised, a signed original copy of the authorised form and subsequent review, renewal and cancellation forms must be kept secure with the investigation file, and a copy of the authorisation and subsequent, reviews, renewals and cancellations must be kept by the PA to the Executive Director Economy & Environment in accordance with document retention guidelines.

1.10 In terms of monitoring e-mails and Internet usage, it is important to recognise important interplay and overlaps with the Council's e-mail and internet policies and guidance, the Telecommunications (lawful business practice) (Interception of Communications) Regulations 2000, the Data Protection Act 1998 and associated guidance. Under normal circumstances the Council's e-mail and internet policies should be used, as any surveillance is likely to be more relevant under the contract employment terms and conditions as opposed to RIPA.

2. Legislative Background

2.1 The Regulation of Investigatory Powers Act 2000 was introduced to provide a comprehensive and coherent framework within which public authority enforcement services could undertake covert investigations lawfully. The 2000 Act provides a regime within which enforcement services may undertake covert activities which infringe some of the, 'qualified rights', such as the right to privacy, or interference with a person's private or family life, granted to individuals via the Human Rights Act 1998 (HRA). Infringement of such rights is only lawful where public authorities can show that it is necessary to protect the public interest and the level of infringement is proportionate to the public interest issue concerned. Compliance with the Regulation

of Investigatory Powers Act was designed to ensure that investigatory actions were HRA compliant.

2.2 The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012, SI 2012/1500 ("the 2012 Order"), was made on 11 June 2012 and came into force on 1 November 2012. Directed Surveillance will be made subject to a new Serious Crime Test. The test is that the criminal offence which is sought to be prevented or detected is punishable, whether on summary conviction or on indictment, by a maximum term of at least 6 months of imprisonment, or would constitute an offence under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933.

2.3 Information obtained about individuals under the 2000 Act is subject to controls and safeguards provided by the Data Protection Act 1998 in relation to the acquisition, processing and distribution of Personal Data. The 1998 Act provides exceptions to the non-disclosure of personal data where it is necessary for the investigation of criminal activities and such data should only be disclosed to organisations outside the Council in accordance with the 1998 Act and the Criminal Procedure and Investigations Act 1996.

2.4 The monitoring of employees' working activities by managers to ensure compliance with the Council's legal, financial and Personnel procedures generally falls outside the 2000 Act. The Council however, as a telecommunications system provider, is permitted under specific legislation to monitor use of its telephone, e-mail and internet access systems provided to employees for use in transacting the Council's business.

2.5 The following sections address detailed provisions for the differenct types of activity covered by this Code.

3. Surveillance

3.1. Types of Surveillance

3. 1.1 'Surveillance' includes:

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

3.1.2. Overt Surveillance

Most of the surveillance carried out by the Council will be done overtly - there will be nothing secretive, clandestine, or hidden about it. In many cases officers will be behaving in the same way as a normal member of the public (e.g. in the case of most test purchases), and/or will be going about Council business openly (e.g. a market inspector walking through markets).

Similarly, surveillance will be overt if the subject has been told it will happen (e.g. where a noisemaker is warned (preferably in writing) that noise will be recorded if noise continues.)

3.1.3 Covert Surveillance

Covert Surveillance is carried out in a manner calculated to ensure that the person subject to the surveillance is unaware of it taking place. (Section 26(9)(a) of RIPA). It cannot, however, be "necessary" if there is reasonably available overt means of finding out the information desired.

RIPA regulates three types of covert surveillance, Directed Surveillance, Intrusive Surveillance and the use of Covert Human Intelligence Sources (CHIS).

3.1.4 Directed Surveillance

Directed Surveillance is surveillance which:-

- is covert;
- is not intrusive surveillance;
- is not carried out in an immediate response to events which would otherwise make seeking authorisation under the Act unreasonable, e.g. spotting something suspicious and continuing to observe it; and
- is undertaken to the purpose of a **specific investigation** or operation in a manner **likely to obtain private information** about an individual (whether or not that person is specifically targeted for the purposes of an investigation). (Section 26(10) of RIPA)

3.1.5 Intrusive Surveillance

This is surveillance that is:-

- covert;
- relates to residential premises and/or private vehicles; and involves the presence of a person in the premises or in the vehicle or is carried out by a surveillance device in the premises/vehicle. Surveillance equipment mounted outside the premises will not be intrusive, unless a device consistently provides information of the same quality and detail as might be expected if they were in the premises/vehicle.

This form of surveillance cannot be carried out or approved by the Council. Only the police and other law enforcement agencies are permitted to use such powers. Likewise, the Council has no statutory powers to interfere with private property.

3.1.6 Surveillance and Social Media

Covert surveillance may be undertaken by a variety of means, wider than personal direct observation of an activity or target. This can include the use of cameras or audio

recording equipment as well as monitoring of records and advertisements. In particular the OSC guidance draws the attention of public authorities to the relevance of RIPA to surveillance undertaken by means of monitoring social networking sites (SNS).

The availability of computers makes surveillance of SNS easy. However, it is important that investigating officers and authorising officers understand the different networks, how they work and how services are provided. It is the responsibility of individuals setting up accounts to make use of the site's privacy settings. Where these are not utilised and information is posted as "open source", there is no expectation of privacy. Consequently RIPA authorisation will not normally be required. However, where viewing of open source sites is repeated or systematic, they this may constitute directed surveillance necessitating authorisation and such activity should be considered on a case by case basis.

On the other hand where a person has set privacy settings which require approval for any individual to view, then accessing this information covertly is likely to require authorisation where the necessity and proportionality test are met. Where the establishment and maintenance of a relationship is required, then it will be necessary to obtain authorisation as a Covert Human Intelligence Source (CHIS). More detail on these provisions is in section 3.1.7 of this policy below. Use of a false identity is not unlawful, but needs to be authorised. However, adoption of the identity of another person must only be undertaken with that person's express permission. Where that person is known or likely to be known to the subject under investigation consideration of the risks to that person and appropriate protective measures which may need to be deployed.

Further guidance on this activity is contained on the OSC procedures paragraph 289.[1]

3.1.7 Use of CHIS A covert human intelligence source (CHIS) is the use or conduct of someone "undercover" who establishes or maintains a personal or other relationship with a surveillance subject for the covert purpose of obtaining information. An Authorising Officer must be satisfied that the CHIS is necessary, that the conduct authorised is proportionate to what is sought to be achieved and that arrangements for the overall management and control of the undercover officer are in force. A CHIS is defined as:

- Someone who establishes or maintains a personal or other relationship for the covert purpose of helping the covert use of the relationship to obtain information.
- RIPA does not normally apply in circumstances where members of the public volunteer information to the Council as part of their normal civic duties, or to contact numbers set up to receive information. (When an informant gives repeat information about a suspect or a family and it becomes apparent that the informant may be obtaining that information in the course of a family or neighbourhood relationship, it probably means that the informant is in reality a CHIS. Information received from such an informant should be referred to legal services for advice before acting on that information.)

The Conduct or Use of a CHIS requires prior authorisation.

[1] https://osc.independent.gov.uk/wp-content/uploads/2016/07/OSC-Procedures-Guidance-July-2016.pdf

- Conduct of a CHIS - establishing or maintaining a personal or other relationship with a person for the covert purpose of (or is incidental to) obtaining and passing on information.
- Use of a CHIS - actions inducing, asking or assisting a person to act as a CHIS and the decision to use a CHIS in the first place.

The Council can use a CHIS if, and only if, the RIPA policy and procedures, as detailed in this document, are followed. Authorisation for a CHIS can only be granted if it is for the purposes of 'preventing or detecting crime'.

3.1.7.1 Juvenile Sources

Special safeguards also apply to the use or conduct of juveniles, that is, those under 18 years old, as sources. On no occasion should the use or conduct of a CHIS under 16 years of age be authorised to give information against his parents or any person who has parental responsibility for him. In other cases, authorisations should not be granted unless the special provisions contained within The Regulation of Investigatory Powers (Juveniles) Order 2000; SI No.2793 are satisfied. Authorisations for juvenile sources should be granted by those listed in Annex A of the Home Office Codes of Practice. The duration of such an authorisation is one month from the time of grant or renewal (instead of twelve months). For the purpose of these rules, the age test is applied at the time of the grant or renewal of the authorisation.

Authorisations should not be granted unless:

- a risk assessment has been undertaken as part of the application, covering the physical dangers and the psychological aspects of the use of the child.
- the risk assessment has been considered by the Authorising Officer and he or she is satisfied that any risks identified in it have been properly explained.
- the Authorising Officer has given particular consideration as to whether the child is to be asked to get information from a relative, guardian or any other person who has for the time being taken responsibility for the welfare of the child. A child under the age of 16 must never be asked to give information against his or her parents.

Authorisations should not be granted unless the Authorising Officer believes that management arrangements exist which will ensure that there will be, at all times, a person who has responsibility for ensuring that an appropriate adult will be present between any meetings between Council representatives and a CHIS under 16 years of age.

3.1.7 2 Vulnerable Individuals

A vulnerable individual is a person who is or may be in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of himself, or unable to protect himself against significant harm or exploitation. Any individual of this description should only be authorised to act as a CHIS in the most exceptional circumstances. In these cases, Annex A of the Home

Office codes of practice lists the authorising officer for each public authority permitted to authorise the use of a vulnerable individual as a CHIS.

Authorisations should not be granted unless:

- a risk assessment has been undertaken as part of the application, covering the physical dangers and the psychological aspects of the use of the vulnerable individual.
- the risk assessment has been considered by the Authorising Officer and he or she is satisfied that any risks identified in it have been properly explained.
- the Authorising Officer has given particular consideration as to whether the vulnerable individual is to be asked to get information from a relative, guardian or any other person who has for the time being taken responsibility for the welfare of the vulnerable person.

3.1.7.3 Record keeping in relation to CHIS

The following matters are specified for the purposes of paragraph (d) of section 29(5) of the 2000 Act (as being matters particulars of which must be included in the records relating to each source):

(a) the identity of the source;
(b) the identity, where known, used by the source;
(c) any relevant investigating authority other than the authority maintaining the records;
(d) the means by which the source is referred to within each relevant investigating authority;
(e) any other significant information connected with the security and welfare of the source;
(f) any confirmation made by a person granting or renewing an authorisation for the conduct or use of a source that the information in paragraph (d) has been considered and that any identified risks to the security and welfare of the source have where appropriate been properly explained to and understood by the source;
(g) the date when, and the circumstances in which, the source was recruited;
(h) the identities of the persons who, in relation to the source, are discharging or have discharged the functions mentioned in section 29(5)(a) to (c) of the 2000 Act or in any order made by the Secretary of State under section 29(2)(c);
(i) the periods during which those persons have discharged those responsibilities;
(j) the tasks given to the source and the demands made of him in relation to his activities as a source;
(k) all contacts or communications between the source and a person acting on behalf of any relevant investigating authority;
(l) the information obtained by each relevant investigating authority by the conduct or use of the source;
(m) any dissemination by that authority of information obtained in that way; and
(n) in the case of a source who is not an undercover operative, every payment, benefit or reward and every offer of a payment, benefit or reward that is made or

provided by or on behalf of any relevant investigating authority in respect of the source's activities for the benefit of that or any other relevant investigating authority.

3.2 Authorising Officer Responsibilities

3.2.1 The SRO will ensure that a sufficient number of Authorising Officers from each department are suitably trained on RIPA, and this policy, and appointed to act in accordance with this document and the law. A list of designated authorised officers is detailed at **Appendix 2**.

3.2.2 It will be the responsibility of Authorising Officers (who have been duly certified) to ensure that their relevant members of staff are suitably trained as 'Applicants'.

3.2.3 Authorising Officers will also ensure that staff who report to them follow this policy and procedures and do not undertake or carry out any form of surveillance without first obtaining the relevant authorisations in compliance with this document.

3..2.4 Authorising Officers must have regard to any **health and safety issues** that may be raised by any proposed surveillance activity. An Authorising Officer should not approve any RIPA forms, unless they are satisfied that the health and safety of council employees/agents have been suitably addressed and/or any risk is minimised so far as is possible, and proportionate to the surveillance that is being proposed.

3.2.5 Authorising Officers must be familiar with the relevant Codes of Practice issued by the Home Office regarding RIPA.

3.2.6 Prior to any applications being authorised consideration must be given as to how to handle confidential information obtained during a surveillance. Failure to do so may invalidate the admissibility of any evidence obtained.

3.2.7 The Authorising Officer must ensure that proper regard is had to **necessity and proportionality** before any applications are authorised. 'Stock phrases' or ‘cut and paste’ narrative must be avoided at all times, as the use of the same may suggest that insufficient consideration had been given to the particular circumstances of any person likely to be the subject of the surveillance. Any equipment to be used in any approved surveillance must also be properly controlled, recorded and maintained for audit purposes.

3.3 Test Purchases

Carrying out test purchases will not (as highlighted above) require the purchaser to establish a relationship with the supplier with the covert purpose of obtaining information and, therefore, the purchaser will not normally be a CHIS. For example, authorisation would not normally be required for test purchases carried out in the ordinary course of business (e.g. walking into a shop and purchasing a product over the counter). By contrast, developing a relationship with a person in the shop, to obtain information about the seller’s suppliers of an illegal product (e.g. illegally imported products) will require authorisation as a CHIS. Similarly, using mobile hidden recording

devices or CCTV cameras to record what is going on in the shop will require authorisation as directed surveillance. A combined authorisation can be given for a CHIS and also directed surveillance.

3.4. Anti-social behaviour activities (e.g. noise, violence etc)

Persons who complain about anti-social behaviour, and are asked to keep a diary, will not normally be a CHIS, as they are not required to establish or maintain a relationship for a covert purpose. Recording the level of noise (e.g. the decibel level) will not normally capture private information and, therefore, does not require authorisation.

Recording sound (with a DAT recorder) on private premises could constitute intrusive surveillance, unless it is done overtly. For example, it will be possible to record if the noisemaker is warned that this will occur if the level of noise continues. Placing a stationary or mobile video camera outside a building to record anti social behaviour on residential estates will require prior authorisation.

Further guidance on CHIS can be found in the Home Office's Code of Practice on surveillance.

4 Access to Communications Data

4.1 Communications data is defined as information held by communications service providers (CSP) (eg telecom, internet, and postal companies) in relation to the communications made by their customers.

4.2 Local Authorities **cannot** seek to obtain **the content** of any communications made via a communications service provider (CSP) as this is a highly intrusive power restricted to the Security services and Police in relation to serious crime.

4.3 Local Authorities are authorised to obtain data relating to the subscriber or user of a communications service or data relating to the use made of such a service ie volume of usage or frequency of use. Local Authorities cannot obtain 'traffic data' ie the location of a communications via a mobile phone.

4.4 Local Authorities may only obtain communications data for the purpose of the prevention and detection of crime.

4.5 Applications for communication data must be made to a Designated Person within the Authority. The designated person must be independent of the investigation and operations whilst holding the prescribed office as defined by Article 4 of the Regulation of Investigatory Powers (Communications Data) Order 2010. A list of designated persons is contained in appendix 3.

Where the DP is not independent of the investigation, for example in circumstances where an independent DP is not available, the DP must record their justification for undertaking the role must be explicitly stated in their recorded considerations. The SRO must notify the Commissioner on their next inspection of all instances where a DP was used who is not independent of the investigation.

4.6 Prior to an application for access to communications data being made, the investigating officer must consult with the SPOC within NAFN. The application is submitted to the Designated Person within the authority for approval. In granting this, they must take into consideration the following:

- necessity
- proportionality
- unintended consequences
- that the type of communication data being applied for is that which a person of their position may grant
- necessity for any conduct to acquire or obtain the communications data, taking into account the advice of the SPOC

4.7 Once approved by the DP the application must be submitted to judicial approval via the Magistrates Court. If satisfied with the application, the magistrate will complete a judicial order, a copy of which will be provided to the NAFN SPOC who will then submit the request to the CSP.

4.8 Once approved, an authorisation will last for one month, This can be renewed during that period. However, if that time expires, a new authorisation is needed for any subsequent access to data.

5. Confidential Information

5. 1 Special safeguards apply with regard to confidential information relating to legal privilege, personal information and journalistic material. The Authorising Officer and the person carrying out the surveillance must understand that such information is confidential and cannot be obtained. Annex A to the code of practice on covert surveillance states that authorisation of such cases should be made by the Head of Paid Service (Chief Executive) or, in his absence, a Chief Officer. Further guidance is available in the Home Office Codes of Practice.

6. Collateral Intrusion

6. 1 Before authorising surveillance the Authorising Officer should also take into account the risk of intrusion into the privacy of persons other than those who are the direct subjects of the investigation/operation (collateral intrusion). Measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the lives of those not directly connected with the investigation or operation.

6. 2 Those carrying out the surveillance should inform the Authorising Officer if the investigation or operation unexpectedly interferes with the privacy of individuals who were not covered by the authorisation. When the original Authorisation may not be sufficient, consideration should be given to whether the Authorisation needs to be amended and re-authorised or a new authorisation is required.

7. Retention and Destruction of Products of Surveillance and Communications Data

7. 1 Where the product of surveillance and communications data could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with

established disclosure requirements for a suitable time period subject to review; and in accordance with the council's document retention guidelines.

7. 2 There is nothing in RIPA which prevents material obtained from properly authorised surveillance from being used in other investigations. Authorising Officers must ensure, therefore, that arrangements are in place for the handling, storage and destruction of material obtained through the use of covert surveillance. Authorising Officers must also ensure compliance with the appropriate data protection requirements and any relevant codes of practice produced by individual authorities relating to the handling and storage of material.

7.3 The PA to the SRO shall maintain a summary of all authorisations in a central record on behalf of the SRO. Officers must immediately inform the PA to the SRO whenever an authorisation is granted, reviewed, renewed or cancelled and give the PA to the SRO the original form for it to be retained centrally.

7.4 The PA to the SRO shall retain the original authorisation, renewal and cancellation forms for a **period of at least three years** from the ending of the authorisation (six years if financial records are involved).

7.5 All officers involved in any aspect of this procedure will retain and secure records in accordance with the requirements of the Data Protection Act and the Authoritiy's procedures thereunder.

7.6 The master form templates contained in the based on the forms published on the Home Office website. The exception to this is the use of a modified version of the cancellation of surveillance form, as recommended in the OSC inspection report of 9 June 2016. The modification is to include a section for review and comment by the Authorising Officer.

8. Monitoring

8.1 The applicant shall retain ensure the original copies of all records pertaining to an applications for authorisation (including refusals), renewals, reviews and cancellations are given to the PA to the SRO for keeping and entering onto the central register of RIPA applications..

8.2 The Senior Responsible Officer (SRO) will periodically sample check the authorisation records to ensure that this policy and procedure; and the legislation and guidance is being complied with.

8.3 Through the Audit Committee, councillors will consider regular internal reports on use of the Regulation of Investigatory Powers Act (RIPA) 2000 to ensure that it is being used consistently with the council's policy and procedures; and that the policy and procedures remain fit for purpose. Councillors should not, however, be involved in making decisions on specific authorisations.

9. Principles of Surveillance

9. 1 In planning and carrying out covert surveillance, officers shall comply with the following principles:

Lawful Purposes - covert surveillance shall only be carried out when necessary to achieve one or more of the permitted purposes available to local authorities (as defined in the Act). Officers carrying out surveillance shall not cause damage to any property or harass any person.

Necessity - covert surveillance shall only be undertaken where there is no reasonable and effective alternative way of achieving the desired objective (s).

Effectiveness - planned covert surveillance shall be undertaken only by suitably trained or experienced officers, or under their direct supervision.

Proportionality - the use and extent of covert surveillance shall not be excessive, i.e. it shall be proportionate to what is sought to be achieved by carrying it out. Officers must consider all alternative ways of obtaining the required evidence. Covert surveillance should be a last resort.

Intrusive surveillance - no activity shall be undertaken that comes within the definition of 'intrusive surveillance', i.e. if it is surveillance of anything taking place on residential premises or in private vehicles **and** involves the presence of an officer on the premises or in the vehicle, or is carried out by means of a surveillance device.

Collateral intrusion - reasonable steps shall be taken to minimise the acquisition of information about persons who are not the subject of the surveillance. The Authorising Officer will review all collateral material which is obtained during an investigation, and any material not relevant to the investigation will be destroyed immediately. Collateral material relevant to the investigation will be retained with the other case material and will be destroyed in line with current procedures.

Risk to Staff - Authorising Officers shall have regard to possible risks to staff, based upon a risk assessment in accordance with the Council's Health & Safety Policy, Directorate safety procedures and/or statutory regulations including any approved code of practice arising from the Health and Safety at Work etc. Act 1974. This shall include an assessment of those risks associated with any premises being used for surveillance. They shall also have the same level of regard to risks to any person acting as CHIS or who has allowed officers to use their identity.

Authorisation - all directed surveillance shall be authorised in accordance with the procedures described below.

10. Authorisation Procedures

10. 1 **Directed Surveillance** and the use of a CHIS can only be lawfully carried out if properly authorised, and in strict accordance with the terms of the authorisation.

Forms can only be signed by Authorising Officers as listed in **Appendix 2**. This Appendix will be kept up to date by the SRO, and will be added to as required. If a Chief Officer wishes to add, delete or substitute a post, he/she must refer such a

request to the SRO for consideration, as necessary. The SRO has been duly authorised to add, delete or substitute posts listed in appendix 2.

Authorisations under RIPA are separate from any delegated authority to act under the Council's scheme of delegations and internal departmental schemes of delegation. All RIPA authorisations, save for authorisations to collect communications data under section 22(3), are for specific investigations only and must be reviewed, renewed or cancelled once a specific surveillance is complete or about to expire.

Current RIPA forms are set out on the Home Office website and should be used as a basis for our application forms.

Directed Surveillance the **Conduct** and **Use** of CHIS and/or disclosure of communications data notices can be authorised by the Council **only on the grounds of preventing or detecting crime**. **No other grounds are available to local authorities.**

10.2 Assessing the Application Form

Any officer giving an authorisation for use of directed surveillance must be satisfied that:

- the authorisation is in accordance with the law.
- the nature of the surveillance and the detail of how it is to be conducted has been fully specified on the application form.
- account has been taken of the likely degree of intrusion into the privacy of persons other than those directly implicated in the operation or investigation ("collateral intrusion"). Measures must be taken, wherever practicable, to avoid and necessary intrusion into lives of those affected by collateral intrusion.
- authorisation is necessary.
- the authorised surveillance is proportionate and the required evidence could not be obtained in any other way.

The Authorising Officer will record on the application form, comments detailing reasons for the authorisation being granted or refused.

The Authorising Officer shall review all authorisations at intervals to be determined by the Authorising Officer and set a review date at the time of the initial application. The review period may be reassessed at each review or renewal of an application. Details of the review and the decision reached should be recorded on the appropriate review form. The results of the review should be recorded on the central record of Authorisations. Any person entitled to authorise may renew Authorisations. Authorisations may be renewed more than once, provided they continue to meet the criteria for authorisation.

Where an authorisation ceases to be either necessary or appropriate the Authorising Officer must cancel the authorisation using the appropriate cancellation form. Authorisations must be cancelled as they do not "die" on the expiry date.

For Communications and CHIS applications, the Authorising Officer should:

- set a date for review of the authorisation, and review on that date using the relevant form;
- allocate a unique reference number for each form;
- ensure that any RIPA central register is duly completed, and that a copy of the RIPA Forms (and any review/renewal/cancellation of the same) are forwarded to the SRO, within one week of the relevant authorisation, review, renewal, cancellation or rejection;
- if the Authorising Officer is unsure of any matter in respect of such applications he/she should seek further advice from the Head of Internal Audit or Monitoring Officer before signing any forms.

On reviewing the canvellation of surveillance form, the Authorising Officers should give consideration to making a direction on the handling of the product as per the OSC guidance. A flow chart outlining the process for the approval of Communications Data Applications is given in appendix 4. A flow chart outlining the process for the approval of Covert Human Intelligence Sources (CHIS) Applications is given in appendix 5.

11. Time Periods and Limitations

11.1 Written authorisations for directed surveillance can only be granted for **three months**, and 12 months for a CHIS. However, whether the surveillance is carried out/conducted or not, in the relevant period, does not mean the 'authorisation' is 'spent'. The Forms do not expire and have to be reviewed, renewed and/or cancelled.

11.2 Notices/Authorisations issued under section 22 RIPA 2000 compelling disclosure of Communications Data are only valid for one month, but can be renewed for subsequent periods of one month, at any time.

11.3 Authorisations can be renewed in writing before the maximum period of the Authorisation has expired. The Authorising Officer must consider the matter afresh, including taking into account the benefits of the surveillance to date, and any collateral intrusion that has occurred. An Authorisation cannot be renewed after it has expired. In such an event, a fresh Authorisation will be necessary.

12. Oversight and Complaints

12. 1 The Office of Surveillance Commissioners (OSC) provides independent oversight of the use of the powers contained within the Regulation of Investigatory Powers Act 2000. This oversight includes inspection visits by Inspectors appointed by the OSC.

12.2 The Regulation of Investigatory Powers Act 2000 establishes an independent Tribunal. This Tribunal has full powers to investigate and decide any cases within its jurisdiction.

Appendix 1 (to the original policy)

The Magistrates' Approval Process

1. The first stage will be to apply for an internal authorisation in the usual way. Once it has been granted, the local authority will need to contact the local Magistrates Court to arrange a hearing. For communications data, the investigating officer must consult with NAFN before applying to the court.

2. The hearing is a 'legal proceeding' and therefore local authority officers need to be formally designated to appear, be sworn in and present evidence or provide information as required by the JP. It is envisaged that the investigating officer will be best suited to fulfill this role..

3. The local authority will provide the JP with a copy of the original RIPA authorisation or notice. This forms the basis of the application to the JP and should contain all information that is relied upon. In addition, the local authority will provide the JP with two copies of a partially completed judicial application/order form.

4. The hearing will be in private and heard by a single JP who will read and consider the RIPA authorisation or notice and the judicial application/order form.

5. The JP will consider whether he or she is satisfied that at the time the authorisation was granted or renewed or the notice was given or renewed, there were reasonable grounds for believing that the authorisation or notice was necessary and proportionate. In addition they must be satisfied that the person who granted the authorisation or gave the notice was an appropriate designated person within the local authority and the authorisation was made in accordance with any applicable legal restrictions, for example that the crime threshold for directed surveillance has been met.

6. Serious Crime Test The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012, SI 2012/1500 ("the 2012 Order"), was made on 11 June 2012 and will also come into force on 1 November 2012. Directed Surveillance will be made subject to a new Serious Crime Test.

7. The order section of the above mentioned form will be completed by the JP and will be the official record of his/her decision. The local authority will need to retain a copy of the form after it has been signed by the JP.
The JP may decide to –

- Approve the grant or renewal of an authorisation or notice
- Refuse to approve the grant or renewal of an authorisation or notice
- Refuse to approve the grant or renewal and quash the authorisation or notice

8. An approval is also required if an authorisation to use such techniques is being renewed. In each case, the role of the JP is to ensure that the correct procedures have been followed and the relevant factors have been taken account of. There is no requirement for the JP to consider either cancellations or internal reviews.

Appeals

A local authority may only appeal a JP's decision on a point of law by making an application for judicial review in the High Court.

Appendix 2 **(to the original policy)**

List of Authorised Officer Posts for Authorising Directed Surveillance

Post	Scope of Authorisation
Head of Law	Applications for miscellaneous and any application in an urgent situation or absence of primary authorising officer as listed below Applications pertaining to a non-criminal investigation into the conduct of an employee (non RIPA)
Director of Public Health	Applications from regulatory services and Safer Walsall Borough Partnership – where the council is the lead agency Applications for covert human intelligence source (CHIS) except in the case of juvenile / vulnerable adults in which case Annex A of the relevant Home Office Codes of Practice apply.
Head of Business Change Systems Leader (Money, Home, Job)	Applications from Benefits

Appendix 3

List of Designated Persons for Granting Authorisations for Accessing Communications Data

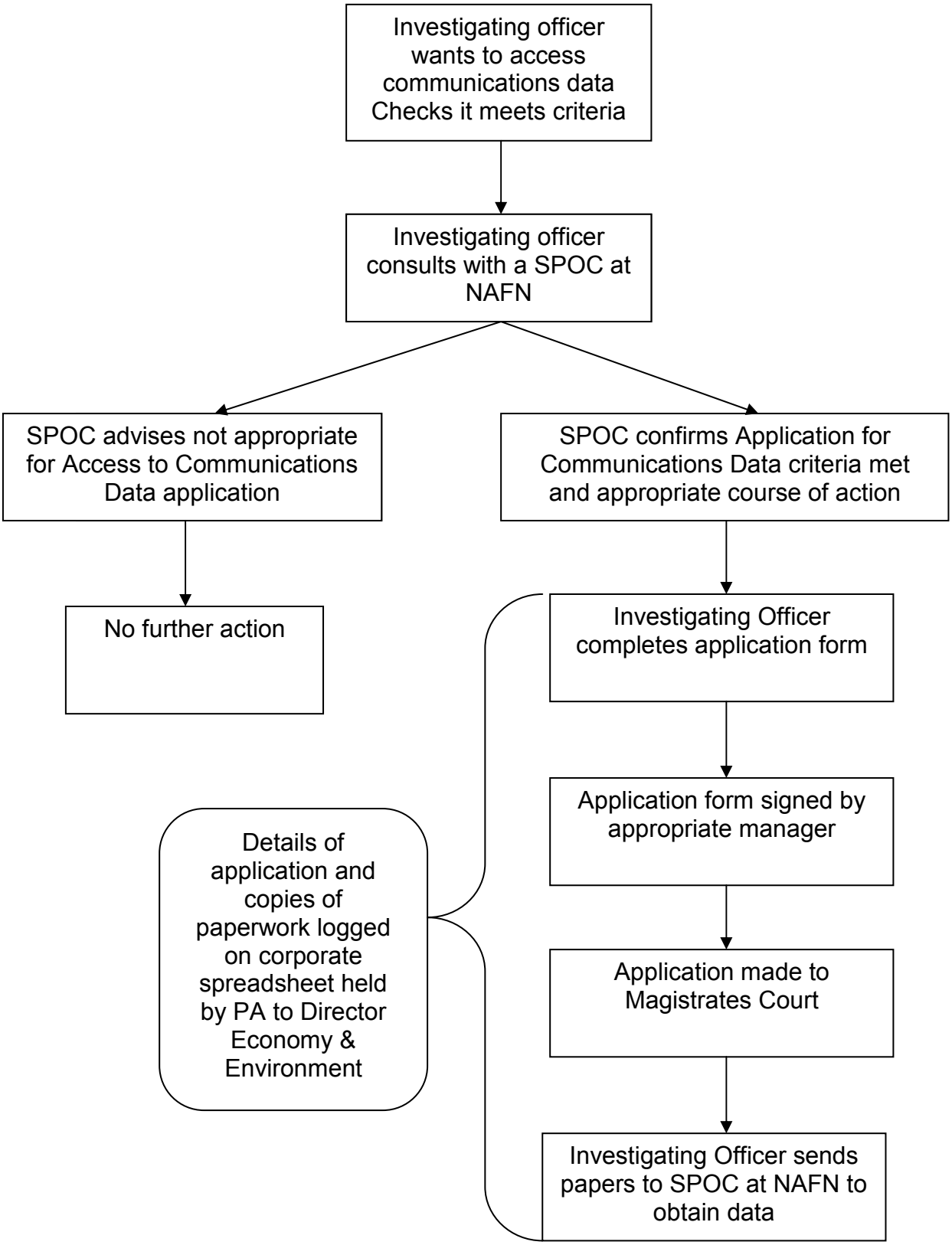
The persons listed below are designated persons for the purposes of authorisations for access to communications data:

An officer who is not in the service area of the investigation should be used.

Post	Name of officer
Regulatory Services Manager Community Protection	Lorraine Boothman
Regulatory Services Manager Business & Compliance	David Elrington
Head of ICT	Carol Williams

Appendix 4

Flow Chart for Approval of Communications Data Applications



Appendix 5

Flow Chart for Approval of Covert Human Intelligence Sources (CHIS) Applications