

Council – 23 February 2012

Regulation of Investigatory Powers Act (RIPA) Policy & Procedures 2012

1. Summary of report:

Following a process of consultation and consideration by the Corporate Management Team and Audit Committee, approval is sought for the new Corporate Policy and Procedures on the Regulation of Investigatory Powers Act (RIPA) 2000. The new procedures replace the previous corporate procedure on directed surveillance dated 2009.

2. Recommendations:

- 2.1 That the Corporate Policy and Procedures on the Regulation of Investigatory Powers Act (RIPA) 2000 appended to this report be approved.
- 2.2 That the Executive Director – Neighbourhood Services be granted delegated authority to make minor amendments to these Policy and Procedures, as required, in consultation with the Head of Legal and Democratic Services.

3. Background

The Regulation of Investigatory Powers Act is the law governing the use of covert techniques by public authorities. It requires that when public authorities – such as local authorities– need to use covert techniques to obtain private information about someone, they do it in a way that is necessary, proportionate, and compatible with human rights.

Where there is an interference by a local authority with the right to respect for private and family life guaranteed under Article 8 of the European Convention on Human Rights and where there is no other source of lawful authority, the consequence of not obtaining an authorisation under the 2000 Act may be that the action is unlawful by virtue of section 6 of the Human Rights Act 1998.

The Home Office has strongly recommended that local authorities seek an authorisation where the surveillance is likely to interfere with a person's Article 8 rights to privacy by obtaining private information about that person, whether or not that person is the subject of the investigation or operation. Obtaining an authorisation ensures that the action is carried out in accordance with law and subject to stringent safeguards against abuse.

Directed surveillance authorisations under Part II of the Regulation of Investigatory Powers Act (RIPA) 2000 may be granted in relation to covert surveillance undertaken in relation to a specific investigation or operation which is likely to result in the obtaining of private information about a person, and which is other than an immediate response to events or circumstances.

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

The council's procedure on directed surveillance was last reviewed in 2009. The new corporate policy and procedures on the Regulation of Investigatory Powers Act (RIPA) 2000 replaces these and is appended to this report.

The policy and procedures have been rewritten to incorporate the requirements of the new codes of practice and the recommendations made following the last Office of the Surveillance Commissioner's Inspection, which took place in March 2010. The key changes are:

- the Senior Responsible Officer's roles and responsibilities;
- procedures for where such surveillance pertaining to a non-criminal investigation into the conduct of an employee is required;
- greater detail regarding procedures for covert human intelligence sources;
- the role of members, particularly that of Audit Committee; and
- key personnel changes of officers with authorising responsibilities.

The new policy and procedures were presented to Corporate Management Team on 12 January 2012; and Audit Committee on 30 January 2012, who recommend that these now be presented for approval by Council.

5. Resource and legal considerations:

Material obtained through covert surveillance may be used as evidence in criminal proceedings. The proper authorisation of surveillance, following an agreed policy and procedure, will ensure the admissibility of such evidence under the common law, S78 of the Police and Criminal Evidence Act 1984 and the Human Rights Act 1998.

6. Citizen impact:

Compliance with the corporate policy and procedures document on the Regulation of Investigatory Powers Act (RIPA) 2000 assists in protecting the council and its officers and provides an assurance to stakeholders about the security of the council's operations.

7. Performance and risk management issues:

The corporate policy and procedures document on the Regulation of Investigatory Powers Act (RIPA) 2000 assists in ensuring positive outcomes in future inspections and that evidence collated is lawful.

8. Equality Implications:

None arising from this report.

9. Consultation:

Officers from legal, regulatory services, internal audit and benefits have been consulted.

Background papers:

Corporate Policy and Procedures on the Regulation of Investigatory Powers Act (RIPA) 2000 appended to this report.

Signed:



Date: 15 February 2012

Jamie Morris
Executive Director, Neighbourhood Services
(Senior Responsible Officer - RIPA)

☎ 01922 653203

✉ morrisj@walsall.gov.uk



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

February 2012



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 - Neighbourhoods.

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 Offices Code of Practices on Covert Surveillance and Covert Human Intelligence Sources 2010. These procedures should be read in conjunction with the Home Offices Codes of Practice. Covert surveillance should be used only rarely and in exceptional circumstances. Copies of the Home Offices 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.
- 1.2 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 Neighbourhoods, 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 Neighbourhoods 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.
- 1.3 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. Where such surveillance pertaining to a non-criminal investigation into the conduct of an employee is required, officers will be required to complete the appropriate forms as detailed at **Appendix 1**, and then forward the form to an Authorising Officer for their approval. For purposes of consistency, such authorisations will last for three months and appropriate action must be taken to review, renew and cancel authorisations. These forms are also detailed at appendix 1. The authorising officer will apply the same criteria as if the request was for RIPA authorisation. For all RIPA authorisations, the forms as detailed on the Home Office web site will be used: <http://www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/ripa-forms>.
- 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 regularly 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.

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 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.
- 2.3 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.

3. Authorising Officer Responsibilities

- 3.1 The SRO will ensure that a sufficient number of Authorising Officers from each department are suitably trained on RIPA, and this policy, and

the appointed to act in accordance with this document and the law. A list of designated authorised officers is detailed at **Appendix 2**.

- 3.2 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'.
- 3.3 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.
- 3.4 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.
- 3.5 Authorising Officers must be familiar with the relevant Codes of Practice issued by the Home Office regarding RIPA.
- 3.6 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.
- 3.7 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.

4. Types of Surveillance

4.1 '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).

Surveillance can be overt or covert.

4.2. **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, or where a premises licence is issued subject to conditions, and the license holder is told the officers may visit without notice or identifying themselves to the owner/proprietor to check that the conditions of the premises licence are being complied with.)

4.3 **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 the 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).

4.3.1 **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)

4.3.2 **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.

4.3.3 Covert Human Intelligence Source

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.

Who is a CHIS?

- 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 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.

What must be authorised?

The Conduct or Use of a CHIS require prior authorisation.

- 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 CHIS's If and only if, the RIPA policy and procedures, as detailed in this document, are followed. Authorisation

for CHIS's can only be granted if it is for the purposes of 'preventing or detecting crime or of preventing disorder'.

Record keeping

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.

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.

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.

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.

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, at:

www.homeoffice.gov.uk/crimpol/crimreduc/regulation/codesofpractice.html

4.4 **Access to Communications Data: Part 1 Chapter II**

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.

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.

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.

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

A notice under section 22(4) of the Act must be issued to the CSP to request them to disclose the data, the forms to do so are stipulated and can be found on the Home Office web site at www.homeoffice.gov.uk/counter-terrorism/regulation-investigatory-powers/ripa-forms

Engagement with CSP's can only be undertaken by Single Point of Contacts (SPOC) who are registered with the Home Office. There are 2 registered SPOCs in the Trading Standards Service.

Benefits utilise the service provided by NAFN (National Anti Fraud Network) who are also registered SPOCs.

Control of this procedure is under the Acquisition and Disclosure of Communications Data, code of practice. This relates to the powers and duties conferred or imposed under Chapter 2 of Part 1 of the Regulation of Investigatory Powers Act 2000 relating to the acquisition of communications data by public authorities and its disclosure by communications service providers. It provides guidance on the procedures to be followed for the acquisition of communications data and describes communications data. It sets out rules for the grant of authorisations to acquire data, the giving of notices to require disclosure of data and the keeping of records, including records of errors.

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 begin 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

- 7.1 Where the product of surveillance could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with established disclosure requirements for a suitable 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 Head of Internal Audit shall maintain a summary of all authorisations in a central record on behalf of the SRO. Authorising Officers must immediately update this record whenever an authorisation is granted, reviewed, renewed or cancelled. The central record of authorisations should be retained for a **period of at least 3 years** from the ending of the authorisation (6 years if financial records are involved).
- 7.4 The Authorising Officer shall retain the original authorisation and renewal forms and cancellation forms for a period of at least 3 years after cancellation, (6 years if financial records are involved).
- 7.5 The master form templates contained in the appendices of this policy and procedure are subject to document control and shall be reviewed annually and, as determined to be necessary.

8. Monitoring

- 8.1 An Authorising Officer shall retain all applications for authorisation (including refusals), renewals, reviews and cancellations.
- 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 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.

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.

10.2 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.

10.3 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. Authorisations to collect communications data under section 22 (3) have, as with section 22 notices, a lifespan of one month. However they can be renewed by serving a new authorisation or notice for further months, within any time during the current life of the notice in question.

10.4 Only the RIPA forms set out on the Home Office website are permitted to be used. Any other forms used, will be rejected by the authorising officer and/or by the SRO.

10.5 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 or preventing disorder.
No other grounds are available to local authorities.

11. Assessing the Application Form

11.1 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.

11.2 The Authorising Officer shall review all authorisations at intervals to be determined by the Authorising Officer, 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. (see appendices). 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.

11.3 Where an authorisation ceases to be either necessary or appropriate the Authorising Officer will cancel the authorisation using the appropriate cancellation form.

11.4 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 1 week of the relevant authorisation, review, renewal, cancellation or rejection;
- in the case of notices relating to communications data, these will be kept by a SPOC designated by the SRO, who will have access to such forms as and when required;

- 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.

12. Time Periods and Limitations

- 12.1 In exceptional circumstances urgent authorisations may be given orally if the time that would elapse before a written authorisation can be granted would be likely to endanger life or jeopardise investigation or operation for which the authorisation was being given. Such oral authorisations expire after 72 hours, and must be confirmed in writing as soon as practicable.
- 12.2 All urgent authorisations must be promptly entered onto the central register at the earliest opportunity. Furthermore, a contemporaneous note of the case made out, by the applicant to the Authorising Officer, to authorise the surveillance must be recorded, as this represents an important aspect of the documentary evidence in relation to the case.
- 12.3 Written authorisations for directed surveillance can only be granted for **3 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.
- 12.4 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.
- 12.5 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

13. Oversight and Complaints

- 13.1 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.
- 13.2 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.



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

Public Authority (including address)	
--	--

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

DETAILS OF APPLICATION
1. Give rank or position of authorising officer
Has a pre-surveillance risk assessment been carried out? Yes <input type="checkbox"/> No <input type="checkbox"/>

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

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

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

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

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

6. Identify why surveillance is necessary in this particular case:

Unique Reference Number	
----------------------------	--

7. Explain why this directed surveillance is necessary in this particular case:

8. Supply details of any potential collateral intrusion and why the intrusion is unavoidable. Describe precautions you will take to minimise collateral intrusion.

9. Explain why this directed surveillance is proportionate to what it seeks to achieve. How intrusive might it be on the subject of surveillance or on others? And why is this intrusion outweighed by the need for surveillance in operational terms or can the evidence be obtained by any other means?

10. Confidential Information. [Code paragraphs 3.1 to 3.12]

INDICATE THE LIKELIHOOD OF ACQUIRING ANY CONFIDENTIAL INFORMATION:

11. Applicant's Details

Name (Print)		Tel No.	
Grade / Rank		Date	
Signature			

Unique Reference Number	
----------------------------	--

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

I hereby authorise as follows:

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

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

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

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

14. (Confidential Information Authorisation.) Supply detail demonstrating compliance with Home Office Codes of Practice relating to this issue.

Expiry of authorisation (3 months from the date / time of authorisation unless otherwise stated here)	
---	--

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

Unique Reference Number	
-------------------------	--

Authorising Officer Name (Print)		Job Title	
Signature		Date and time	
Expiry date and time [e.g. authorisation granted on 1 April 2005 – expires on 30 June 2005, 23.59]			

15. Urgent Authorisation Authorising officer to explain why they considered the case so urgent that an oral instead of written authorisation was given.				
Name (Print)		Job Title:		
Signature		Date and Time		
Urgent authorisation Expiry date:		Expiry time:		
<i>Remember the 72 hour rule for urgent authorities</i>	e.g. authorisation granted at 5pm on June 1 st expires 4.59 on 4 th June			

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

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

Unique Reference Number	
-------------------------	--



Walsall Council

Review of a Directed Surveillance authorisation
**REVIEW OF DIRECTED SURVEILLANCE AUTHORISAION IN
RELATION TO EMPLOYEES**
THIS IS NOT A RIPA REVIEW FORM
**THIS FORM SHOULD NOT BE USED FOR REVIEWING RIPA
SURVEILLANCE**

Public Authority (including address)	
---	--

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

Details of review:

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

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

Unique Reference Number	
------------------------------------	--

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

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

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

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

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

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

Unique Reference Number	
------------------------------------	--

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

10. Date of next review.	
---------------------------------	--

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

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

Unique Reference Number	
----------------------------	--



Walsall Council

APPLICATION FOR RENEWAL OF A DIRECTED SURVEILLANCE IN RELATION TO EMPLOYEES

(PLEASE ATTACH A COPY OF THE ORIGINAL AUTHORISATION)

THIS IS NOT A RIPA RENEWAL FORM

**THIS FORM SHOULD NOT BE USED FOR AUTHORISING RIPA
RENEWALS**

Public Authority (including address)	
---	--

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

Details of renewal:

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

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

Unique Reference Number	
------------------------------------	--

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

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

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

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

7. Applicant's Details

Name (Print)		Tel No.	
Grade / Rank		Date	
Signature			

Unique Reference Number	
----------------------------	--

8. Authorising Officer's Comments. This box must be completed.

9. Authorising Officer's Statement

I, [insert name], hereby authorise renewal of the directed surveillance/operation as detailed above.
The renewal of this authorisation will last for 3 months unless renewed in writing.

This authorisation will be reviewed frequently to assess the need for the authorisation to continue.

Name (Print)

Job Title

Signature

Date

Renewal From:

Time:

Date:

Date of first review.

**Date of subsequent reviews for this
authorisation.**

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

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



Walsall Council

**CANCELLATION OF A DIRECTED SURVEILLANCE
AUTHORISATION IN RELATION TO EMPLOYEES
THIS IS NOT A RIPA AUTHORISATION FORM
THIS FORM SHOULD NOT BE USED FOR AUTHORISING RIPA
SURVEILLANCE**

Public Authority (including full address)	
---	--

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

Details of cancellation:

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

2. Explain the value of surveillance in the operation:

3. Authorising Officer's statement:		
I [insert name], hereby authorise the cancellation of the directed surveillance/operation as detailed above.		
<table border="0"> <tr> <td>Name (Print)</td> <td>Job Title</td> </tr> </table>	Name (Print)	Job Title
Name (Print)	Job Title	
<table border="0"> <tr> <td>Signature</td> <td>Date</td> </tr> </table>	Signature	Date
Signature	Date	

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

5. Authorisation cancelled.	Date:	Time:
------------------------------------	--------------	--------------

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

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



List of Designated Authorised Officer Posts

Post	Scope of Authorisation
Head of Internal Audit Head of Law	Applications for miscellaneous and any application in an urgent situation Applications pertaining to a non-criminal investigation into the conduct of an employee (non RIPA)
Regulatory Manager	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 Benefits	Applications from Benefits