Shropshire Council

REGULATION OF INVESTIGATORY POWERS POLICY

USE OF COVERT DIRECTED SURVEILLANCE
USE OF COVERT HUMAN INTELLIGENCE SOURCES
ACQUISITION OF COMMUNICATIONS DATA

Approved by Shropshire Council on:
Adopted by Shropshire Council on:

CONTENTS

PART A : BACKGROUND

Part A sets out the background to the use of covert investigatory techniques by Shropshire Council ('the Council') under the provisions of the Regulation of Investigatory Powers Act 2000 (RIPA).

1. Introduction

1.1 The primary aim of Central and Local Government enforcement work is to protect the individual, the environment and a variety of groups such as clients, consumers and workers. At the same time, carrying out enforcement functions in a fair, practical and consistent manner helps to grow and promote a prosperous and thriving national and local economy. The Council is committed to these aims and to maintaining a fair and safe society.

1.2 On occasions, in the course of enforcement work to ensure regulatory compliance, fulfil the Council's statutory duties and achieve predetermined outcomes, it may become necessary for the Council to undertake the use of covert investigatory techniques. RIPA sets out the regulatory framework to control the use of these techniques by public authorities. RIPA does not provide powers to carry out covert activities; it provides a defence against accusations of a breach of the Convention on Human Rights (ECHR) and regulates the conduct of Council officers who undertake such activities in a manner that ensures compatibility with the ECHR, particularly Article 8 that deals with the right to respect for private and family life.

1.3 RIPA specifically permits the Council to use three covert techniques for the purposes of preventing or detecting crime or preventing disorder. These are covert directed surveillance, the use of covert human intelligence sources (CHIS) and the acquisition of communications data.

1.4 However, RIPA does not prohibit the use of these techniques for purposes other than the prevention or detection of crime or preventing disorder. Consequently, the Council may legally use covert techniques for purposes other than those defined in RIPA. Where the techniques are used for non RIPA defined purposes, the Council shall have due regard to the principles of RIPA, the Codes published by the Home Office and its own RIPA guidance and, in practice, apply these as if the purposes for which the techniques are being used do fall within the RIPA regime.

1.5 Covert directed surveillance is undertaken in relation to a specific investigation or operation where the person or persons subject to the surveillance are unaware that it is or may be taking place. This may result in the Council obtaining private information about persons, which may or may not be for the purposes of the specific investigation. However, the Council cannot undertake covert surveillance in residential premises or private vehicles.

1.6 CHIS are undercover officers, public informants or, in some cases, people/officers who make test purchases. Such sources may be used by the

Council to obtain or pass on information about another person without their knowledge as a result of establishing or making use of an existing relationship. This clearly has implications for the invasion of a person's privacy and is an activity that is strictly regulated by the legislation.

1.7 The acquisition of communications data is where the Council acquires the who, when and where of communication but not the what, i.e. not the content of what was said or written. The Council may obtain service user information and subscriber information. This includes, for example, the type of communication, time sent, the duration and billing information such as the name, address and bank details of the subscriber of telephone and internet services.

1.8 These covert investigatory techniques play a necessary part in modern life. They are used not only to target criminals in order to prevent and detect crime and disorder but also as a means of protecting the public from harm.

1.9 The covert techniques controlled by RIPA form part of the duties of many law enforcement officers and other public bodies. Within the Council, service areas/functions that may undertake investigations include, but are not limited to, regulatory services, environment, education welfare, housing, social care, council tax, benefits, outdoor recreation and internal audit. All these service areas/functions may, at some point, need to utilise covert techniques as part of their official duties to effectively deliver service and Council outcomes.

1.10 For example, Council officers may need to covertly observe the activities of businesses and individuals and/or form covert relationships as part of their enforcement functions to verify the legality of the supply of goods or services including for the purposes of preventing and detecting underage sales of alcohol and/or tobacco. It may be necessary to obtain subscriber details for mobile phone numbers to track down individuals involved in consumer related doorstep crime. It may also be necessary to covertly observe the activities of individuals who are suspected of serious controlled waste offences or serious/serial council tax and benefit fraud or other serious crime or fraudulent activity such as theft of money or assets. Covert observation of Council employees may also be undertaken to verify compliance with employment contracts and for disciplinary purposes. During these and other types of investigations it may be necessary to record the activities of individuals using covert recording equipment.

1.11 To provide independent oversight in respect of the way in which investigatory techniques are utilised, RIPA has put in place the Office of Surveillance Commissioners (OSC), the Interception of Communications Commissioner's Office (IOCCO) and the Investigatory Powers Tribunal (IPT). This is because RIPA activities may give rise to interference with an individual's privacy and consequently the Council must consider its obligations under Article 8 of the ECHR.

PART B : POLICY STATEMENT

Part B sets out the policy adopted by the Council in respect of its use of covert investigatory techniques under the provisions of RIPA.

2. Policy Statement

2.1 This policy is intended to demonstrate that covert directed surveillance, CHIS and the acquisition of communications data will only be used to obtain information or evidence when no other investigation method or technique will deliver the required outcomes.

2.2 All residents and businesses within Shropshire will benefit from this policy as it provides the framework for the Council to effectively implement RIPA to ensure human rights are protected when enforcing criminal legislation; in particular, it sets out how the Council intends to limit intrusion into the personal activities of individuals. The policy assists the Council to identify and take action to reduce the level of crime in the community.

2.3 The Council shall not undertake any covert techniques referred to in Part A paragraph 1.3 ('covert techniques') of this policy without the prior authorisation from a trained senior officer who has the delegated power to grant such authorisation (i.e. a designated person under Sections 22, 28 and/or 29 of RIPA) **AND** where the covert techniques are used for the purposes of preventing or detecting crime or for preventing disorder an order approving the authorisation has been granted by a Justice of the Peace (JP)[1].

2.4 The Council shall authorise the use of covert directed surveillance under RIPA for the purpose of preventing or detecting crime only where the investigation relates to criminal offences that are punishable by a maximum term of at least six months imprisonment or are related to specified criminal offences for underage sales of alcohol or tobacco. This 'crime threshold' does not apply to the authorisation of a CHIS or to the acquisition of communications data.

2.5 The Council shall authorise the use of a CHIS or the acquisition of communications data for the purposes of preventing or detecting crime or of preventing disorder.

2.6 The Council may authorise the use of covert techniques for purposes other than those specified in RIPA.

2.7 Unless there are unequivocal and undeniably compelling reasons (having considered necessity, proportionality and the anticipated level of collateral intrusion) to authorise the use of covert techniques to investigate disorder that does not involve criminal offences or to investigate offences relating to littering, dog control, fly-posting or noise nuisance, the Council shall not authorise the use of any covert techniques to investigate such matters.

[1] **Attention is drawn to the provisions of Statutory Instrument 2012 No. 2563 (L.9); the Magistrates' Courts (Regulation of Investigatory Powers) Rules 2012, where an application is not made in a criminal case.**

2.8 In addition, authorising officers/designated persons must believe that the covert technique(s) is/are necessary and proportionate to what it/they seek(s) to achieve. In making this judgement, officers shall consider whether the information may be obtained using any other methods and also ensure sufficient steps are in place to reduce the impact of the covert techniques on other people who are not the subject of the operation or investigation (collateral intrusion). If authorising officers/designated persons do not believe that the covert technique(s) is/are necessary and proportionate to what it/they seek(s) to achieve **or** if other methods may be used to obtain the information **or** insufficient steps are in place to reduce collateral intrusion, officers shall not grant authorisation.

2.9 Authorisations shall, except in an emergency, be made in writing and contain the details required by the relevant sections of RIPA and the relevant associated Codes of Practice (the Codes)[2] issued by the Secretary of State pursuant to Section 71 of RIPA.

2.10 The Council cannot and shall not, under any circumstances, authorise 'intrusive surveillance', the acquisition of communications data referred to as 'traffic data', the interception of communications, the investigation of protected electronic information or property interference. Authorising officers/designated persons shall not grant authorisation to any officer to undertake these activities.

2.11 In addition, the Council shall ensure that:-

a) there is a designated person ('the senior responsible officer') within the Council who has specific responsibility for the Council's enforcement activities under RIPA;

b) there is a designated person ('the RIPA co-ordinator') within the Council who has specific responsibility for drafting the Council's RIPA policy and practical guidance and holding, maintaining and updating the centrally retrievable record of all authorisations issued and any subsequent renewals, reviews and cancellations of those authorisations;

c) a suitable pool of officers are designated to present RIPA cases to JPs under Section 223 of the Local Government Act 1972;

d) corporate practical guidance is issued on the use of covert directed surveillance, the use of CHIS and the acquisition and disclosure of communications data;

e) all officers charged with the responsibility of being an authorised officer/designated person are appropriately supported and trained;

[2] **Code of practice on the acquisition and disclosure of communications data (March 2015); Code of practice on covert surveillance and property interference (December 2014); Code of practice on the use of covert human intelligence sources (December 2014); and any subsequent revisions of these codes or new codes that may from time to time be issued**

f) all officers charged with the responsibility of conducting covert directed surveillance, using a CHIS or acquiring communications data are appropriately supported and trained; and

g) all officers dealing with complaints are aware that the Investigatory Powers Tribunal (IPT) has been introduced to examine complaints about the inappropriate use of covert investigatory techniques and the infringement of human rights that may result from inappropriate use.

2.12 Where investigations are carried out for any purpose that falls outside the RIPA regime, e.g. for the purposes of investigating internal Council disciplinary matters or where the 'crime threshold', as referred to in paragraph 2.4 above, is not met, the Council may still use the covert techniques described in RIPA. In such circumstances, judicial approval is not required.

2.13 To ensure that covert techniques used in line with paragraph 2.12 above are used in a manner that is compatible with the ECHR, the Council shall have due regard to the principles of RIPA, the Codes published by the Home Office, and its own RIPA guidance and, in practice, apply these as if the purposes for which the techniques are being used do fall within the RIPA regime.

2.14 When considering the authorisation of covert techniques, the facts of each investigation or operation involving the techniques shall be individually considered on their specific merits.

PART C : PRACTICAL GUIDANCE

Part C sets out the practical guidance that the Council requires all officers to follow when using any of the covert investigatory techniques controlled by RIPA.

3. Introduction

3.1 The purpose of this guidance is:-

a) to explain beyond the policy statement, where necessary, the scope of RIPA and the circumstances where it applies in respect of Council activities;

b) to provide additional general guidance where the Codes do not cover matters that the Council wants to provide guidance on or where specific matters would benefit from further emphasis; and

c) to provide guidance on the judicial approval process.

3.2 The Council has had full regard to the Codes when preparing this guidance.

3.3 The content of the Codes has largely not been repeated in this guidance other than to emphasise a small number of specific issues. This is on the basis that all officers within the Council, when involved with covert directed surveillance, using a CHIS and/or acquiring communications data, are required to refer to, familiarise themselves with and follow the guidance provided in the appropriate and current Code(s). The Codes are admissible in evidence in any criminal and civil proceedings. They are available on the GOV.UK website (https://www.gov.uk/government/collections/ripa-codes).

4. Scope of RIPA

4.1 RIPA provides the statutory basis for local authorities and other organisations to authorise and use covert techniques. It was introduced to protect individuals' human rights whilst also ensuring that law enforcement and security agencies have the investigatory techniques they need to carry out their roles effectively.

4.2 The Council is included within the framework of RIPA with regard to the authorisation of covert directed surveillance, the use of CHIS and for the purposes of authorising the acquisition of communications data.

4.3 It is permissible to undertake these investigatory covert techniques only when relevant criteria are satisfied and the use of the techniques are authorised by an officer with delegated powers. Such authorisation gives lawful authority to carry out the covert techniques.

4.4 Obtaining authorisation helps to protect the Council and its officers from complaints of interference with the rights protected by Article 8 (1) of the ECHR which is now enshrined in English law through the Human Rights Act 1998. This is because the interference with the private life of citizens will be 'in accordance with the law'. In addition, the activities undertaken must also be

necessary and proportionate. Provided activities undertaken are in accordance with the law and a judgement has been made that they are necessary and proportionate they will not be in contravention of human rights legislation.

4.5 Only officers at Service Manager level or above may be given delegated powers to act as the Council's authorised officers/designated persons.

4.6 Only the Head of Paid Service (or any person acting on his/her behalf) has the power to authorise the use of a vulnerable individual or a juvenile as a CHIS. A person may only act on behalf of the Head of Paid Service in exceptional absence circumstances. The provision is not intended to allow ad hoc persons to grant such authorisations.

4.7 Routine patrols, observation at trouble 'hotspots', immediate response to events and the overt use of CCTV are all techniques that do not generally require authorisation. However, attention must be paid to the guidance provided in respect of these techniques in the relevant Code.

5. Additional general guidance

5.1 Council members shall set and/or agree continuance of this policy and the guidance, as appropriate. Where it is agreed by the Senior Responsible Officer (SRO), in consultation with the Portfolio Holder for Regulatory Services, Housing and Commissioning (Central), that RIPA is being used consistently within the policy and that the policy remains fit for purpose then the policy may continue to operate without wider consideration or revision by Council members. However, where there are any concerns about the manner in which RIPA is being used or that the policy is not fit for purpose, the SRO shall take appropriate steps to address these concerns, including revising the policy, in accordance with relevant Council procedures.

5.2 The use of RIPA by Council officers shall be reported to members of the Audit Committee on a regular basis and to the Council, as appropriate, to ensure that RIPA is being used consistently within the policy and that the policy remains fit for purpose.

5.3 Refer to **Appendix 1** for persons designated by the Council as:-

- the SRO
- the RIPA Co-ordinator
- officers with delegated powers to grant authorisations under Sections 22, 28 and 29 of RIPA (Note: officers are permitted to grant authorisations across the Council and are not restricted to granting authorisations within their specific service area but before being permitted to grant authorisations, they must have undergone appropriate RIPA training)
- officers with delegated powers to present RIPA cases to JPs under Section 223 of the Local Government Act 1972 (Note: additional officers may be given such delegated powers, as required, in accordance with the Council's Scheme of Delegation)

5.4 Monitoring of authorisations may be undertaken by the SRO or by a suitably trained officer under the direction of the SRO. All Council officers shall provide such assistance as is required to enable effective monitoring to be undertaken.

5.5 The RIPA Co-ordinator is responsible for maintaining the Council's 'Central Register of Authorisations'. RIPA records shall be retained for a minimum period of 5 years. After the minimum retention period has expired, the RIPA Co-ordinator shall arrange for secure destruction of the records unless it is believed that the records may be relevant to pending or future legal proceedings, in which case they shall be retained for a suitable further period, commensurate with any subsequent review.

5.6 Deciding when authorisation is required involves making a judgement and doing so with the support of the guidance in the relevant Codes and any additional guidance that is made available. Where officers are in any doubt they shall seek the advice of an authorising officer/designated person. Where the authorising officer/designated person is in any doubt they shall seek advice from the Head of Legal and Democratic Services.

5.7 Only the Head of Paid Service (or any person acting on his/her behalf) and the Head of Legal and Democratic Services have the power to authorise directed surveillance involving any Council member. A person may only act on behalf of the Head of Paid Service in exceptional absence circumstances. The provision is not intended to allow ad hoc persons to grant such authorisations.

5.8 Appropriate risk assessments must be carried out before authorisations are granted. See **Appendix 2** for an example, but note this will not cover all aspects of the actual operation being authorised.

5.9 Unless renewed or cancelled, and providing they do not relate to urgent oral authorisations or written authorisations granted by a person who is permitted to act only in urgent cases, the duration of authorisations are:-

- Covert directed surveillance — 3 months
- CHIS — 12 months (1 month if CHIS under 18)
- Communications data — 1 month from the date of JP's approval

NB The expiry time on all authorisations is always at 23:59, e.g. an authorisation granted on 1 April 2015 at 16:54 will expire on 30 June 2015 at 23.59.

5.10 Renewals shall be authorised and approved by a JP prior to the expiry of the original authorisations; but they run from the expiry date/time of the original authorisations. Authorisations may be renewed more than once if still considered necessary and proportionate and approved by a JP. Applications for renewals shall not be made until shortly before the original authorisation period is due to expire but officers shall take account of factors that may delay the renewal process such as intervening weekends and the availability of an authorising officer/designated person and a JP.

5.11 Authorising officers/designated persons shall set authorisation review dates at the outset of the process and ensure these are undertaken regularly.

5.12 A review of an authorisation is not the same as a renewal and authorising officers/designated persons are directed to paragraph 5.10 above and the relevant parts of each of the Codes to ensure the difference is fully understood and the principles correctly applied.

5.13 Authorising officers/designated persons shall formally and promptly cancel authorisations once the authorised covert activity has served its purpose or has become unnecessary or disproportionate.

5.14 In order to ensure that authorising officers/designated persons have sufficient information to make informed decisions, and to provide the OSC and the IOCCO with appropriate information, detailed records shall be made and retained by the Council.

5.15 To facilitate record keeping, the forms to be completed are those that are available on the GOV.UK website (https://www.gov.uk/government/collections/ripa-forms--2). For covert directed surveillance and CHIS the forms are entitled:-

Covert Directed Surveillance

- Application for the use of directed surveillance
- Renewal of directed surveillance
- Cancellation of the use of directed surveillance
- Review of the use of directed surveillance

Covert Human Intelligence Sources

- Application for the use of Covert Human Intelligence Sources
- Renewal of authorisation to use Covert Human Intelligence Sources
- Cancellation of Covert Human Intelligence Sources
- Reviewing the use of Covert Human Intelligence Sources

5.16 Where covert techniques are used for purposes other than those defined under RIPA and in accordance with paragraphs 2.12 and 2.13 above, the forms to be completed are those referred to in **Appendix 3**.

5.17 With respect to the acquisition of communications data, all applications shall be made electronically via the National Anti-Fraud Network (NAFN) website (www.nafn.gov.uk) and all associated records retained by NAFN. In addition, authorising officers/designated persons must provide the RIPA co-ordinator with sufficient details of the communications data authorisations to enable the details, as required by the relevant Code, to be entered onto the Council's 'Central Register of Authorisations'.

5.18 Where errors occur in respect of the acquisition of communications data, and they are not errors made by NAFN, these errors must be reported by an

authorising officer/designated person to the IOCCO using the appropriate form available on the GOV.UK website. The form is entitled:-

- Reporting an error by a public authority to the IOCCO

5.19 It is the responsibility of authorising officers/designated persons to ensure all **original** applications (including refusals) and associated renewals, reviews and cancellations are forwarded to the RIPA Co-ordinator. This does not apply to the acquisition and disclosure of communications data as the original records are retained by NAFN. However, sufficient details of communications data authorisations shall be forwarded to the RIPA Co-ordinator to enable the 'Central Register of Authorisations' to be completed.

5.20 Where the Codes refer to 'confidential material', any advice or guidance required in line with the provisions of the Codes shall be sought from the Head of Legal and Democratic Services.

5.21 Where investigatory activity is likely to involve both covert directed surveillance and the use of a CHIS, RIPA practice permits the two types of authorisations to be legally combined onto one form. However, it is the Council's practice for separate forms to be completed to maintain the distinction between the two techniques being used.

5.22 In cases of joint working where other agencies are involved on the same operation, authority for covert techniques shall be obtained from the Council's authorising officers/designated persons. Authorisation cannot be granted by the authorising officer/designated person of another agency for the actions of Council officers and vice versa.

5.23 All covert recording equipment shall be stored securely to prevent unauthorised use. A log must be created and maintained to record the date/time the equipment was removed from storage, by whom, for what purpose and the date/time it was returned to storage and by whom.

5.24 Where recording equipment is to be used covertly, this shall be specifically detailed in the relevant RIPA application to ensure the use of the equipment is properly authorised by an authorising officer/designated person.

5.25 All RIPA generated material shall be processed in accordance with Council guidance relating to data protection requirements, the handling, storage, retention and destruction of confidential material.

5.26 Where material is obtained through any activity covered in this guidance, which is wholly unrelated to a criminal or other investigation or to any person who is not the subject of the investigation, and there is no reason to believe it will be relevant to future criminal or civil proceedings, it must be destroyed immediately. The decision as to whether or not unrelated material should be destroyed is the responsibility of the relevant authorising officer/designated person.

5.27 Nothing in RIPA prevents material obtained through the proper use of the authorisation procedures on one investigation from being used in another investigation; however, the use outside the Council of any material obtained by means of the activities covered in this guidance and, other than in pursuance of the grounds on which it was obtained, shall only be authorised in the most exceptional circumstances.

5.28 Authorising officers/designated persons shall take account of any guidance[3] issued by the OSC and IOCCO and properly promote and make it accessible to all relevant officers within the Council.

6. Judicial approval process

6.1 With regard to the judicial approval process for RIPA, all officers involved in the authorisation process shall familiarise themselves with the latest guidance available for local authorities in England and Wales as detailed in the Codes and published on the GOV.UK website (https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/118173/local-authority-england-wales.pdf) and follow the guidance contained therein.

6.2 The Council deems investigating officers, supported by authorising officers/designated persons, to be best able to answer any questions posed by JPs on the policy and practice of conducting covert operations as well as the detail of the actual cases under investigation. It is not necessary to use a solicitor to make the case to a JP.

6.3 Authorising officers/designated persons shall contact Her Majesty's Courts and Tribunals Service (HMCTS) administration team at the appropriate Magistrates' Court to arrange a hearing and investigating officers shall attend the hearing and where, required, be accompanied by authorising officers/designated persons.

6.4 The application and judicial order forms to be used for judicial approval are produced at **Appendix 4**.

6.5 For the purposes of the acquisition of communications data, the completed judicial order shall be provided to the NAFN Single Point of Contact (SPoC).

6.6 Where covert techniques are used for purposes other than those defined under RIPA and in accordance with paragraphs 2.12 and 2.13 above, there is no requirement to obtain judicial approval.

6.7 Further guidance and information is made available by the OSC and the IOCCO on their websites – refer to the links below. Officers shall ensure they consider and have regard to such information as appropriate.

[3] **OSC Procedures and Guidance – Oversight arrangements for covert surveillance and property interference conducted by public authorities and to the activities of relevant sources (December 2014); and any subsequent revision of this and any other guidance that may from time to time be issued**

- https://osc.independent.gov.uk/
- http://www.iocco-uk.info/

APPENDIX 1

1. **Senior Responsible Officer:** Paul McGreary, Head of Business Support and Regulatory Services

2. **RIPA Co-ordinator:** Frances Darling, Senior Commissioner, Business Support and Regulatory Services

3. **Officers with delegated powers to grant authorisations under Sections 22, 28 and 29 of RIPA** (subject to appropriate RIPA training)**:-**

   Clive Wright, Head of Paid Service
   Claire Porter, Head of Legal and Democratic Services
   Paul McGreary, Head of Business Support and Regulatory Services
   Frances Darling, Senior Commissioner, Business Support and Regulatory Services
   Martin Key, Operations Manager Environmental Protection and Resolution
   Karen Collier, Operations Manager Health and Community Protection
   Ian Kilby, Operations Manager Planning Services
   Philip Wilson, Service Delivery Manager Business Support, Learning & Skills Group
   Timothy Sneddon, Operations Manager Environmental Maintenance
   Tina Russell, Head of Safeguarding
   Maria White, Service Manager Assessment and Early Help
   Steve Ladd, Service Manager Placements
   Sarah Wilkins, Service Manager Early Help
   Christine Kerry, Team Manager Education Access Service
   Philip Weir, Revenues & Benefits Service Manager
   Deborah Hughes, Shropshire Outdoor Partnerships Manager
   Ruth Houghton, Head of Social Care, Efficiency and Improvement

4. **Officers with delegated powers to present RIPA cases to JPs under Section 223 of the Local Government Act 1972:-**

   Clive Wright, Head of Paid Service
   Claire Porter, Head of Legal and Democratic Services

Paul McGreary, Head of Business Support and Regulatory Services
Frances Darling, Senior Commissioner, Business Support and Regulatory Services
Martin Key, Operations Manager Environmental Protection and Resolution
Karen Collier, Operations Manager Health and Community Protection
Ian Kilby, Operations Manager Planning Services
Phil Wilson, Service Delivery Manager Business Support, Learning & Skills Group
Timothy Sneddon, Operations Manager Environmental Maintenance
Carmen Eccleston, Street Scene Manager
Grant Tunnadine, Investigation and Targeted Intervention Team Manager
Anthony Coffey, Public Protection Officer
Sally Jones, Public Protection Officer
Andrew Bishop, Public Protection Officer
Stacy Arnold, Public Protection Officer
Charlotte Smith, Public Protection Officer
Fiona Gee, Public Protection Officer
Mark Southern, Planning and Enforcement Officer
Melanie Durant, Planning and Enforcement Officer
Julian Beeston, Planning and Enforcement Officer
Tina Russell, Head of Safeguarding
Maria White, Service Manager Assessment and Early Help
Steve Ladd, Service Manager Placements
Sarah Wilkins, Service Manager Early Help
Martin Hearle, Team Manager
Pam Ralph, Team Manager
Kathryn Shenton, Team Manager
Jill Carpenter, Team Manager
Christine Kerry, Team Manager - Education Access Service
Lindsey Glover, Education Welfare Team Leader
Joanne Smith, Education Welfare Officer
Samantha Edwards, Education Access Officer
Jane Parsons, Education Welfare Officer
Philip Weir, Revenues & Benefits Service Manager

Jessica Taylor, Benefits Manager
Claire Penrose, Partnership Liaison Officer
Brian Allman, Business Rates Manager
Paul Newns, Senior Visiting Officer
Ben Castree, Visiting Officer
Mary Edge, Visiting Officer
Deborah Hughes, Shropshire Outdoor Partnerships Manager
Shona Butter, Mapping and Enforcement Team Leader
Lucy McFarlane, Rights of Way Officer – Legal Orders and Enforcement
Emily Harrison, Rights of Way Officer – Legal Orders and Enforcement
Ruth Houghton, Head of Social Care, Efficiency and Improvement

5. **Officers with delegated powers to grant authorisations for purposes other than those specified under RIPA** (subject to appropriate RIPA training)**:-**

All officers listed at 3 above.
James Walton – Head of Finance, Governance & Assurance

APPENDIX 2

Regulation of Investigatory Powers Act 2000

Example risk assessment, guidance and equipment checklist

Note: All forms of surveillance should be carried out by properly trained or experienced officers – in particular only those that can demonstrate competency through training or experience in vehicle or other forms of mobile surveillance should carry out such activities.

Task/Description	Hazard/Risk	Preventative measures	Operation checks
Covert Surveillance: General Guidance: 1. Follow Regulation of Investigatory Powers Act 2000 procedures. 2. Always consider the safety of officers and the general public when carrying out any of the above activities. 3. If you feel that you have been recognised but the operation is not compromised then cease activities. If however there is any possibility that the operation may have been compromised, stand down the entire	The hazards faced by operatives are more often verbal rather than actual physical violence. However physical violence is always a danger particularly with more serious offences.	1. Always ensure you have the local Police office telephone number entered into your mobile phone. 2. Withdraw from confrontational situations if the Police are not present. 3. Where possible familiarise yourself with the location, target and any activities you are expecting to encounter. 4. Always ensure that your management are aware of your activities and when you expect to return. Report regularly at predetermined times to another officer.	· Carry and use surveillance logs. · Ensure you and your witnesses have notebooks, credentials and pens with them. · Keep a schedule for reporting to the office or control. · Carry communications equipment

team and reconsider the operation.			

Task/Description	Hazard/Risk	Preventative measures	Operation checks
Covert Surveillance: Static From fixed premises (e.g. a house or building)	Personal injury: 1. From possible attack by individuals if discovered. 2. En route to or from or at premises 3. Condition of premises – poorly lit or dangerous or from structural or electrical faults 4. Slips, trips and falls especially in old disused premises and on stairs Note: Attack can be from individuals under surveillance, their associates or from members of the public. Members of the public will be unaware of your purpose and are likely to be sympathetic towards the target.	1. Familiarise yourself with the area and identify all access and escape routes – do not use same route every time 2. Never work on your own and have team members close by with a view of the premises to alert of any danger 3. Follow established techniques for surveillance or adapt as necessary to suit local conditions. 4. Keep doors and access to the building locked from the inside. 5. Ensure you have adequate communication (e.g. radio and/or mobile phone - important to ensure you can contact the police from your chosen communications equipment). 6. Ensure communications equipment can transmit and receive from premises - during the operation carry out a periodic communication check. 7. Report regularly to a contact outwith the premises. 8. Ensure equipment is suitable – use covert radios if noise will be a problem; mute all phone tones and rings. 9. Pre-alert the Police if you feel they might be needed and have a contact number for them. 10. Be aware that any form of noise (including toilets	· Brief all participants on locations and operational details. · Ensure all personnel know their positions and that of other colleagues. · *Ensure you know how to operate the equipment correctly* · Check all batteries are charged and take back-up batteries if possible. · Make sure you have sufficient media (e.g. tape/ film). · Complete a 'dry run' beforehand if required.- check if premises have power(saves batteries) and check condition of premises for security and

		flushing) from 'disused' premise may alert others to your presence and compromise the operation. 11. Leave premises as you find them. Do not leave any signs that you have been there. 12. Use furnished premises if possible as less noise is transmitted if the property has floor coverings.	comfort and identify any potential dangers · Ensure all communications equipment is working and establish alternative communications in poor reception areas • Ensure comfort break facilities are available and note that different genders have different requirements.

Task/Description	Hazard/Risk	Preventative measures	Operation checks
Covert Surveillance: Static From a vehicle (e.g. surveillance van)	Discovery of operative leading to violence. Fear of discovery and isolation (This may be applicable to all forms of surveillance.) Road accident Increased potential for discovery from noise levels or movement within the vehicle	In addition to the measures above: 1. Ensure the vehicle has enough fuel and is adequately ventilated 2. Follow established techniques for surveillance or adapt as necessary to suit local conditions. 3. Ensure the vehicle does not cause an obstruction on the road; do not park in a poorly lit or dangerous location. 4. Keep all doors locked during operation. 5. The driver should be seen to walk away from vehicle but should be close by if required. 6. Ensure team members have view of vehicle to advise of any potential dangers 7. Consider whether Police should be aware of your	In addition to above: · Ensure provision is made for comfort breaks. · Ensure that windows are clean if being used for filming or general viewing prior to use.

		location and purpose. 8. Ensure vehicle is prepared for surveillance e.g. one way glass, screens or blacked out windows. 9. If overt surveillance from a car, do not park the car near a school or in a residential area for long periods of time. 10. If overt surveillance from a car, less attention is drawn to a lone occupant in the passenger or rear seat although escape becomes more difficult. 11. Where possible leave the vehicle unattended with surveillance equipment operating.	

Task/Description	Hazard/Risk	Preventative measures	Operation checks
Covert Surveillance: Mobile From a moving vehicle	Attack: 1. Personal attack (road rage) 2. Intentional collision by person under investigation. Road accident: Risk is increased due to style of driving required to carry out this type of 'follow' Remember! RTA – no protection against prosecution for driving without due care and attention, careless driving or	This should not normally be under taken unless officer has appropriate training and is working in a team of similarly experienced officers. There is a major risk to individuals as well as other road users and members of the public including pedestrians. 1. As many vehicles as required should be used from those available. 2. Ensure car is properly maintained and fit for the road 3. Ensure the car has enough fuel, preferably a full tank of petrol. 4. Avoid using a distinctive car that could be identified. Consider using a hired car. 5. Be careful not to be followed into enclosed areas or dead ends and try to keep within view of another officer at all times. 6. Make suitable arrangements for communications 7. Have a plausible story ready as to why you are	In addition to above: · Have roadmaps of area and any areas you may be likely to visit · Be aware of position and deployment of other vehicles in the operation · If using hired car check that insurance is adequate and familiarise yourself with all controls and the performance of the car. · Carry disposable

	dangerous driving. Insurance may not pay for any accident whilst you are engaged in such activities. Roadworks & other obstacles Pedestrians and children	there if challenged or engaged in conversation. 8. Be aware of your environment – not just the target.	camera for record of any collision or damage

Task/Description	Hazard/Risk	Preventative measures	Operation checks
Covert Surveillance: On foot	Confrontation with target Other members of target gang challenging and cutting off retreat route Physical violence from both human and animal Challenge from members of the public	1. Work in a team. 2. Have a plausible story as to why you are there and who you are, if challenged or engaged in conversation. Avoid eye contact with target 3. Be careful not to be followed into enclosed areas or dead ends and try to keep within view of another officer at all times. 4. Have a plausible story ready as to why you are there if challenged or engaged in conversation. 5. Survey the area if possible and make a note of local pitfalls and facilities	In addition to above: Wear appropriate footwear/clothing – have change of clothing available from team member/support vehicle · Have sufficient loose change for fares etc

Task/Description	Hazard/Risk	Preventative measures	Operation checks
Covert surveillance: Illegal waste disposal sites.	Detection on instillation by third party Violence and aggression	1. Always ensure pre reconnaissance check is undertaken prior to instillation of cctv units. 2. Abort instillation if detection is expected. 3. Request road closures where applicable 4. Always leave the scene if confronted	Prepare Site plans of areas Advanced weather forecasts

	Manual handling Adverse weather conditions Attack by animals Stings and bites Slips trips and falls	5. Where possible always work in pairs 6. Always familiarise yourself with object weights before moving 7. Always request help where objects are heavy or awkward to move 8. Park as close to site as possible to avoid unnecessary lifting and carrying 9. Always undertake weather checks prior to instillation 10. Do not enter premises where livestock / animals are kept. 11. Always ensure suitable equipment and training is undertaken before using ladders. 12. Always use PPE provided or where needed 13. Be aware of Injurious plant species if utilising hedges, bushes, plants or trees for CCTV units. (Nettles, Giant hogweed, thorn bushes, etc.) 14. Be aware of wasp and hornet nests when selecting sites for CCTV locations Ensure a first aid kit is close at hand	PPE First aid kit provision

APPENDIX 3

Forms to be used when undertaking covert techniques for purposes other than those specified under RIPA

Covert Directed Surveillance

1. Application for a directed surveillance authorisation
2. Renewal of a directed surveillance authorisation
3. Cancellation of a directed surveillance authorisation
4. Review of the a directed surveillance authorisation

Covert Human Intelligence Sources

5. Application for a Covert Human Intelligence Sources Authorisation
6. Renewal of a Covert Human Intelligence Sources Authorisation
7. Cancellation of a Covert Human Intelligence Sources Authorisation
8. Review of a Covert Human Intelligence Sources Authorisation

Acquisition of communication data

9. Accredited SPoC Notifying IOCCO of a Reportable Error

1

European Convention on Human Rights / Human Rights Act 1998
Application for a Directed Surveillance Authorisation

Public Authority ***(including full 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 in accordance with the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 No. 521. (For local authorities the exact/formal position of the authorising officer must be given.)

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 the grounds upon which the directed surveillance is <u>necessary</u> having regard to RIPA and Shropshire Council internal guidance and procedures.

7. Explain why this directed surveillance is necessary on the grounds you have identified [Code paragraph 3.3].

8. Supply details of any potential collateral intrusion and why the intrusion is unavoidable. [Bear in mind Code paragraphs 3.8 to 3.11.] 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 [Code paragraphs 3.4 to 3.7]?

10. Confidential information [Code paragraphs 4.1 to 4.31]. INDICATE THE LIKELIHOOD OF ACQUIRING ANY CONFIDENTIAL INFORMATION:

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

Signature		

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

I hereby authorise directed surveillance defined as follows: [*Why is the surveillance necessary, whom is the surveillance directed against, Where and When will it take place, What surveillance activity/equipment is sanctioned, How is it to be achieved?]*

13. Explain why you believe the directed surveillance is necessary [Code paragraph 3.3].
Explain why you believe the directed surveillance to be proportionate to what is sought to be achieved by carrying it out [Code paragraphs 3.4 to 3.7].

14. (Confidential Information Authorisation.) Supply detail demonstrating compliance with Code paragraphs 4.1 to 4.31.

Date of first review	

Programme for subsequent reviews of this authorisation: [Code paragraph 3.23]. Only complete this box if review dates after first review are known. If not or inappropriate to set additional review dates then leave blank.

Name (Print)		Grade / Rank		
Signature		Date and time		
Expiry date and time [e.g.: authorisation granted on 1 April 2005 - expires on 30 June 2005, 23.59]				

15. Urgent Authorisation [Code paragraph 5.9]: Authorising officer: explain why you considered the case so urgent th instead of a written authorisation was given.
16. If you are only entitled to act in urgent cases: explain why it was not reasonably practicable for the application to be considered by a fully qualified authorising officer.

Name (Print)		Grade/ Rank		
Signature		Date and Time		
Urgent authorisation Expiry date:		Expiry time:		
Remember the 72 hour rule for urgent authorities – check Code of Practice.	**e.g. authorisation granted at 5pm on June 1st expires 4.59pm on 4th June**			

2

European Convention on Human Rights / Human Rights Act 1998
Renewal of a Directed Surveillance Authorisation

Public Authority ***(including full 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 the renewal.

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

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

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

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

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

Signature	

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

9. Authorising Officer's Statement.
I, [insert name], hereby authorise the 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) _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ Grade / Rank - - - - - - - - - - - - - - - - - - Signature - - - - - - - - - - - - - - - - Date -
Renewal From: Time: Date:

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

European Convention on Human Rights / Human Rights Act 1998
Cancellation of a Directed Surveillance Authorisation

Public Authority ***(including full address)***	

Name of Applicant		Unit/Branch /Division	
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 investigation/operation as detailed above.			
Name (Print)	_____	Grade	_____
Signature	_____	Date	_____

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

5. Authorisation cancelled.	Date:	Time:

4

European Convention on Human Rights / Human Rights Act 1998
Review of a Directed Surveillance authorisation

Public Authority ***(including address)***	

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

Details of review:

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

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

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

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

5. Detail any incidents 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	
Grade/Rank		Date	

Signature	

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

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

10. Date of next review.	

5

European Convention on Human Rights / Human Rights Act 1998
Application for a Covert Human Intelligence Sources (CHIS) Authorisation

Public Authority *(including full address)*	

Name of Applicant		**Service/Department /Branch**	
How will the source be referred to(i.e. what will be his/her pseudonym or reference number)?			
What is the name, rank or position of the person within the relevant investigating authority who will have day to day responsibility for dealing with the source, including the source's security and welfare (often referred to as the Handler)?			
What is the name, rank or position of another person within the relevant investigating authority who will have general oversight of the use made of the source (often referred to as the Controller)?			
Who will be responsible for retaining (in secure, strictly controlled conditions, with need-to-know access) the source's true identity, a record of the use made of the source and the particulars required under RIP (Source Records) Regulations 2000 (SI 2000/2725)?			
Investigation/Operation Name (if applicable)			

DETAILS OF APPLICATION
1. Give rank or position of authorising officer in accordance with the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 No. 521. (For local authorities the exact/formal position of the authorising officer must be given.)*Where appropriate throughout amend references to the Order relevant to your authority.*
2. Describe the purpose of the specific operation or investigation.
3. Describe in detail the purpose for which the source will be tasked or used.
4. Describe in detail the proposed covert conduct of the source or how the source is to be used.
5. Identify on which grounds the conduct or the use of the source is necessary under RIPA or internal Shropshire Council procedures
6. Explain why this conduct or use of the source is necessary on the grounds you have identified [Code paragraph 3.2].

7. Supply details of any potential collateral intrusion and why the intrusion is unavoidable. [Bear in mind Code paragraphs 3.8 to 3.11.] **Describe precautions you will take to minimise collateral intrusion and how any will be managed.**
8. Are there any particular sensitivities in the local community where the source is to be used? Are similar activities being undertaken by other public authorities that could impact on the deployment of the source (see Code paragraphs 3.17 to 3.18)?

9. Provide an assessment of the risk to the source in carrying out the proposed conduct (see Code paragraph 6.14).
10. Explain why this conduct or use of the source is proportionate to what it seeks to achieve. How intrusive might it be on the subject(s) of surveillance or on others? How is this intrusion outweighed by the need for a source in operational terms, and could the evidence be obtained by any other means [Code paragraphs 3.3 to 3.5]?
11. Confidential information [Code paragraphs 4.1 to 4.21] Indicate the likelihood of acquiring any confidential information.
References for any other linked authorisations:

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

13. Authorising Officer's Statement. [Spell out the "5 Ws" – Who; What; Where; When; Why and HOW – in this and the following box.] THE AUTHORISATION SHOULD IDENTIFY THE PSEUDONYM OR REFERENCE NUMBER OF THE SOURCE, NOT THE TRUE IDENTITY.
14. Explain <u>why</u> you believe the conduct or use of the source is necessary [Code paragraph 3.2] **Explain <u>why</u> you believe the conduct or use of the source to be proportionate to what is sought to be achieved by their engagement [Code paragraphs 3.3 to 3.5].**
15. Confidential Information Authorisation. Supply details demonstrating compliance with Code paragraphs 4.1 to 4.21

16. Date of first review:	

17. Programme for subsequent reviews of this authorisation [Code paragraphs 5.15 and 5.16]. Only complete this box if review dates after first review are known. If not, or inappropriate to set additional review dates, then leave blank.

18. Authorising Officer's Details			
Name (Print)		**Grade/Rank/Position**	
Signature		**Time and date granted*** **Time and date authorisation ends**	

**** Remember, an authorisation must be granted for a 12 month period, i.e. 1700 hrs 4th June 2006 to 2359hrs 3 June 2007***

19. Urgent Authorisation [Code paragraphs 5.13 and 5.14]: Authorising Officer: explain why you considered the case so urgent that an oral instead of a written authorisation was given.

20. If you are entitled to act only in urgent cases: explain why it was not reasonably practicable for the application to be considered by a fully designated Authorising Officer

21. Authorising Officer of urgent authorisation				
Name (Print)		**Grade/Rank/Position**		
Signature		**Date and Time**		
Urgent authorisation expiry date:		**Expiry time:**		
Remember the 72 hour rule for urgent authorisations – check Code of Practice [Code Paragraph 5.14]. e.g. authorisation granted at 1700 on 1st June 2006 expires 1659 on 4th June 2006				

6

European Convention on Human Rights / Human Rights Act 1998
Renewal of a Covert Human Intelligence Sources (CHIS) Authorisation

(Please attach the original authorisation)

Public Authority ***(including full address)***	

Name of Applicant		Unit/Branch	
Full Address			
Contact Details			
Pseudonym or reference number of source			
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 the renewal.

3. Detail why it is necessary to continue with the authorisation, including details of any tasking given to the source.

4. Detail why the use or conduct of the source is still proportionate to what it seeks to achieve.

5. Detail the use made of the source in the period since the grant of authorisation or, as the case may be, latest renewal of the authorisation.

6. List the tasks given to the source during that period and the information obtained from the conduct or use of the source.

7. Detail the results of regular reviews of the use of the source.

8. Give details of the review of the risk assessment on the security and welfare of using the source.

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

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

11. Authorising Officer's Statement. The authorisation should identify the pseudonym or reference number of the source not the true identity.

Name (Print)	_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _	Grade / Rank
Signature		Date
Renewal From:	Time:	Date: End date/time of the authorisation

NB. Renewal takes effect at the time/date of the original authorisation would have ceased but for the renewal

Date of first review:	
Date of subsequent reviews of this authorisation:	

European Convention on Human Rights / Human Rights Act 1998
Cancellation of Covert Human Intelligence Sources (CHIS)
Authorisation

Public Authority ***(including full address)***	

Name of Applicant		Unit/Branch	
Full Address			
Contact Details			
Pseudonym or reference number of source			
Investigation/Operation Name (if applicable)			

Details of cancellation:

1. Explain the reason(s) for the cancellation of the authorisation:
2. Explain the value of the source in the operation:

3. Authorising officer's statement. This should identify the pseudonym or reference number of the source not the true identity.			
Name (Print)	_____	Grade	_____
Signature	_____	Date	_____

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

European Convention on Human Rights / Human Rights Act 1998
Review of a Covert Human Intelligence Sources (CHIS) Authorisation

Public Authority *(including full address)*	

Applicant		**Unit/Branch**	
Full Address			
Contact Details			
Pseudonym or reference number of source			
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 information has been obtained and the value of the information so far obtained.

3. Detail the reasons why it is necessary to continue using a Covert Human Intelligence Source.

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

5. Detail any incidents 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. Give details of the review of the risk assessment on the security and welfare of using the source.

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

9. Review Officer's Comments, including whether or not the use or conduct of the source should continue.

10. Authorising Officer's Statement. THE AUTHORISATION SHOULD IDENTIFY THE PSEUDONYM OR REFERENCE NUMBER OF THE SOURCE, NOT THE TRUE IDENTITY.
Name (Print) _ _ _ _ _ _ _ _ _ _ _ _ _ _ Grade / Rank Signature _ _ _ _ _ _ _ _ _ _ _ _ _ _ Date

Date of next review:	

9

European Convention on Human Rights / Human Rights Act 1998
Accredited SPoC Notifying IOCCO of a Reportable Error

An error can only occur after a designated person:

1. Has granted an authorisation and the acquisition of data ha been initiated, or
2. Has given notice and the notice has been served on a CP in writing, electronically or orally

Guidance on errors and those which must be reported to the IOCCO are contained within the code of practice (see in particular paragraph 6.15)

Reportable errors must be brought to the attention of IOCCO within 5 working days of being discovered (see paragraph 6.17 of the code)

1) Name of Accredited SPoC		4) SPoC's Telephone Number	
2) Office, Rank or Position of SPoC		5) SPoC's Fax Number	
3) SPoC's email Address		6) The error can be reported by email to	Ch2.inspectorate@ homeoffice.gsi.gov.uk

7) DETAILS OF THE ERROR
State whether Notice of Authorisation: Describe the communications data applied for as set out on the application; Describe the nature of the error; Date and time the error occurred; Date: Time: If the effort was made by the CSP – Name of the CSP and state whether CSP has been informed:
8) UNINTENDED COLLATERAL INTRUSION
If any has taken place, please describe what it was
9) PREVENTION OF SIMILAR ERRORS REOCURRING
What steps have been, or will be, taken to ensure that a similar error does not reoccur
10) REPORTING OF THE ERROR TO THE COMMISSIONER AND NOTIFYING THE SENIOR RESPONSIBLE OFFICER AND THE DESIGNATED PERSON *Note: There is a requirement to report the error to your senior responsible officer (SRO) and then to the Commissioner*

Details of the SRO	Name of the SRO Telephone No Email address of the SRO
Details of the DP	Name of the DP Telephone No Email address of the DP
The date and time the report has been completed by SPoC	Date Time

APPENDIX 4

Forms to be used when applying for judicial approval under RIPA

1. Application for judicial approval
2. Order

1

APPLICATION FOR JUDICIAL APPROVAL

Insert service area/department
Shirehall,
Abbey Foregate
Shrewsbury
SY2 6ND

Shropshire Council

Application for Judicial Approval for authorisation to obtain or disclose communications data, to use a covert human intelligence source or to conduct directed surveillance

Regulation of Investigatory Powers Act 2000 Sections 23A, 23B, 32A, 32B

Criminal Procedure Rules 2012; Rule 6.27 & 6.28

Local Authority	**Shropshire Council**
Department	**Insert service area/department**
Offence Under Investigation: **(inc. Statute / SI and Section)**	**Insert here the section and Act that you are investigating** **** Note, where the application relates to Directed Surveillance, details must be given of the Offence section and it must be capable of a custodial penalty of at least 6 months. (Excludes Underage sales)**
Address of premises or identity of subject	**Enter premises / person details**

Covert technique requested: **(Tick one box and specify details below)**

Communications Data ☐

Covert Human Intelligence Source ☐

Directed Surveillance ☐

Summary of Details

Insert here details of the investigation / operation. (Note – if looking at communications data, be sure to specify the telephone numbers / IP addresses)

It would prejudice the investigation if the respondent or any other person affected were present.

Note: **This application should be read in conjunction with the attached RIPA Authorisation / RIPA Application or Notice bearing the Investigation Reference Number given below:**

Investigation Reference Number	**Your File Reference**
Investigating Officer	**Name and Job title**
Authorising Officer / Designated Person **Name and Rank**	
Officer(s) appearing before JP	**Name & Job title**
Address of applicant department	**Shropshire Council** **Insert service area/department** **Shirehall** **Abbey Foregate** **Shrewsbury** **Shropshire SY2 6ND**
Contact telephone number	
Contact e-mail address (optional)	
Number of pages	

The applicant states to the best of his/her knowledge and belief that this application discloses all the information that is material to what the Court must decide and the content of this application is true.

Signed : ……

Dated: ……...

2

ORDER

Order made on an application for Judicial Approval for authorisation to obtain or disclose Communications Data, to use a Covert Human Intelligence Source or to conduct Directed Surveillance.

Regulation of Investigatory Powers Act 2000 Sections 23A, 23B, 32A, 32B.

Criminal Procedure Rules 2012: Rule 6.27 & 6.28

Magistrates Court: Shrewsbury Magistrates' Court

Having considered the application, I (tick one)

☐ **Am satisfied that there are reasonable grounds for believing that the requirements of the Act were satisfied and remain satisfied, and that the relevant conditions are satisfied and I therefore approve the grant or renewal of the authorisation / notice.**

☐ **Refuse to approve the grant or renewal of the authorisation / notice.**

☐ **Refuse to approve the grant or renewal and quash the authorisation / notice.**

Notes

……

……

……

Reasons

……

……

……

Signed: ……

Date: …… **Time:** ……

Full Name: ……..

Address of Magistrates' Court: Shrewsbury Magistrates' Court, The Court House, Preston Street, Shrewsbury SY2 5NX