REGULATION OF INVESTIGATORY POWERS ACT 2000 POLICY

Document Control

Document Ref:	RIPA2018	**Date Created:**	Dec 2018
Version:	Draft 5	**Date Modified:**	15/1/2019
Revision due	Dec 2019		
Author:	Paul Anstey	**Sign & Date:**	
Owning Service	Public Protection and Culture (in consultation with Legal Services)		
Equality Impact Assessment: (EIA)	Date undertaken:		
	Issues (if any):		

Chief Executive	Sign & Date:	
Corporate Director (Communities)	Sign & Date:	
Corporate Director (Economy and Environment)	Sign & Date:	

Change History

Version	Date	Description	Change ID
Draft 1	27/12/2018	Review and internal consultation with Peter Northey (Intel and Business Development – PPP) and Sean Murphy (PPP Manager)	
Draft 2	8/01/2019	Further comments from Sarah Clarke (Legal Services) and Peter Northey (PPP)	
Draft 3	8/01/2019	Additional content on Social Network Sites	
Draft 4	15/01/2019	Feedback from IPCO Assistant Commissioner audit	
Draft 5	31/01/2019	Further review from Head of Legal and Head of PPC following IPCO audit	

West Berkshire COUNCIL

Contents

1. Introduction to RIPA

1.1 RIPA is an acronym for the Regulation of Investigatory Powers Act 2000. This Act was introduced to ensure that surveillance and certain other intelligence gathering complies with the European Convention on Human Rights ('The Convention'), importantly Article 8 which provides:

1.1.1 Everyone has the right to respect for his private and family life, his home and his correspondence;

1.1.2 There shall be no interference by any public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

1.2 Article 8 is a qualified right. If the right to respect for one's home, private and family life is interfered with it has to be proportionate and in accordance with the exceptions above.

1.3 Article 6 of The Convention is also applicable. This deals with the right of everyone to a fair and public hearing within a reasonable time by an independent tribunal. This can include the investigative process supporting that process.

1.4 Part II of RIPA provides a statutory framework that is compliant with The Convention when using surveillance techniques. It also introduces national standards that apply to the police and other law enforcement agencies. Local authorities are classified as law enforcement agencies as they are tasked to investigate certain crimes. For example (not exhaustive):

1.4.1 Benefit fraud;

1.4.2 Trading standards offences (running from fraud to animal welfare offences);

1.4.3 Noise nuisance; and

1.4.4 Non-compliance with planning enforcement notices.

1.5 By virtue of Section 48(2) of RIPA, surveillance includes:

1.5.1 Monitoring, observing, listening to persons, their movements, their conversations or their other activities or communications;

1.5.2 Recording anything monitored, observed or listened to in the course of surveillance; and

1.5.3 Surveillance by or with the assistance of a surveillance device.

1.6 The purpose of this policy is to provide certain guidance as regards RIPA as well as identifying key terms. Covert surveillance (that is essentially secret) requires authorisation otherwise the information gathered may not be admissible in court or compensation may be payable for a breach of an individuals human rights.

1.7 The Home Office has published a number of statutory Codes of Practice under RIPA, those relating to surveillance activity permitted by Local Authorities are referenced at Appendix 1.

1.8 The Investigatory Powers Commissioner's Office (IPCO) provides independent oversight of the use of investigatory powers by intelligence agencies, police forces and other public bodies. A range of guidance materials is available via Appendix 2.3. This includes those previously issued by the OSC and the Council will maintain a watching brief on the recommendations coming from the Consolidate Guidance to update the policy as required.

1.9 RIPA only applies to the core functions[1] of the Council. Covert activity undertaken as part of the general functions of the Council will not enjoy the protection of RIPA and are not covered by this document.

1.10 Where an activity takes place that has not been properly authorised, this must be reported to the Senior Responsible Officer (SRO) without delay. The SRO will be responsible for notifying IPCO in accordance with their requirements.

1.11 All nominated Officers are detailed at Appendix 3.

2. Purpose

2.1 The purpose of this policy is to ensure that all covert surveillance carried out by Council employees (Officers) and the use of Covert Human Intelligence Sources (CHIS) is performed in accordance with the law.

2.2 When carrying out such activities Officers must comply with the relevant Code of Practice issued by the Home Office and have regard to any guidance issued by the Commissioner having oversight of that activity.

2.3 Officers must also have regard to guidance published by other bodies and, where they chose to deviate from such guidance, must be able to justify that decision if challenged. The Better Regulation Delivery Office Code of Practice[2] (BRDO Code) on under age sales is one such example.

2.4 The Head of Legal and Head of Public Protection and Culture liaise on the content of this policy and update both the Chief Executive and Corporate Board where appropriate.

3. Applicability

3.1 This Policy applies to:

3.1.1 All employees working for the Council, including those working from home or at non-Council locations.

3.1.2 Other persons including Elected Members, Consultants, Agency staff and Contractors working for the Council, external organisations working with the Council, whilst engaged on Council business .

[1] Investigatory Powers Tribunal (C v The Police and the Secretary of State for the Home Office – IPT/03/32/H of 14.11.2006)

[2] Age Restricted Products and Services: A Code of Practice for Regulatory Delivery – BIS April 2014 https://www.gov.uk/government/publications/code-of-practice-age-restricted-products

3.1.3 All cases where “Directed Surveillance” is being planned or carried out and “Covert Human Intelligence Sources” (CHIS) are used or planned to be used as part of the core function of the Council.

3.2 For clarity, Officers working within the Public Protection Partnership (PPP)[3] are employees of the Council for the delivery of Environmental Health, Licensing and Trading Standards functions across the Bracknell Forest Borough Council and Wokingham Borough Council areas (in addition to the Council area of West Berkshire). This policy applies to the PPP and, where appropriate, the Council consults with its partners on its application and scope.

3.3 It is the responsibility of each Council employee and other person mentioned to familiarise themselves with and adhere to this Policy.

3.4 Adherence to this Policy is a condition of working for the council or using its assets.

3.5 The Head of Legal Services and Head of Public Protection and Culture will consult with Corporate Management Team (CMT) on this Policy where appropriate.

4. Key Terminology for the Policy

4.1 Directed Surveillance

This is defined in S26(2) of RIPA as surveillance which is covert, but not intrusive and undertaken:

4.1.1 For the purposes of a specific investigation or operation; and

4.1.2 In such a manner as is likely to result in the obtaining of private information about a person (whether or not the person is specifically identified for the purposes of the investigation or operation); and

4.1.3 Otherwise than by way of an immediate response to events or circumstances.

4.2 Intrusive Surveillance

4.2.1 Local authorities **CANNOT** conduct intrusive surveillance.

4.2.2 Intrusive surveillance includes:

4.2.2.1 Surveillance involving the presence of an individual or surveillance device on residential premises or in a private vehicle. .

4.2.2.2 Directed Surveillance on certain premises where material subject to legal privilege is likely to be obtained.

4.2.2.3 The use of a CHIS where material subject to legal privilege is likely to be obtained.

[3] http://decisionmaking.westberks.gov.uk/mgCommitteeDetails.aspx?ID=449

4.3 Covert Human Intelligence Source (CHIS)

A CHIS, their conduct, and the use to which they are put is defined within Section 26(7) and (8) of RIPA. Chapter 2 of the relevant Code provides examples of where this regime may apply.

4.3.1 The use of a CHIS involves inducing, asking or assisting a person to engage in conduct for covert purposes or to obtain information by the means of such conduct. A person is a CHIS if they establish or maintain a personal or other relationship with someone else for the covert purpose of facilitating:

4.3.1.1 Using the relationship to obtain information or to provide access to any information to another person; or

4.3.1.2 Covertly disclosing information obtained by the use of or as a consequence to another person; or

4.3.1.3 Covertly disclosing information obtained by the use of, or as a consequence of, the existence of such a relationship;

4.3.2 A relationship for a covert purpose is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose. This may include those participating in test purchase operations;

4.3.3 Circumstances where unsolicited information is provided to the Council (e.g. through the Consumer Advice or Action Fraud portals) will not normally be viewed as information obtained through the use of a CHIS. However, Officers must be aware that such information may have been obtained in the course of an ongoing relationship with a family member, friend or business associate. The Council has a duty of care to all members of the public who provide information to us and appropriate measures must be taken to protect that source;

4.3.4 Once in receipt of this unsolicited information, Officers must consider carefully if or how they approach the provider to seek clarification or further information. An attempt to solicit further information may be deemed as “inducing, asking or assisting” and bring the informant within the definition of a CHIS. See appendices for more detail.

4.3.5 Where a CHIS application is completed, consideration should be given as to whether a Directed Surveillance Application is also required or whether all the surveillance activity contemplated can be dealt with in a single CHIS application.

4.4 Private Information

4.4.1 The likelihood of obtaining Private Information is a key consideration when undertaking Directed Surveillance. Officers must be able to demonstrate that they have a clear understanding of this concept and, where covert activities have been undertaken without a Directed Surveillance authorisation, they must be able to justify that decision.

4.4.2 RIPA (s26(2)(b)) makes it clear that considerations to the likelihood of obtaining private information should not be restricted to the target of the surveillance, collateral intrusion and the risk of obtaining private information from those not connected with the activity must be considered. Private information includes any aspect of a person's private or personal relationships with others, including family and business relationships. See appendices for more detail.

5. The Need for Authorisation

5.1 Whenever it is proposed to conduct Directed Surveillance or to use a Covert Human Intelligence Source an authorisation should be sought under Part II of RIPA.

5.2 All Authorising Officers shall be trained and have attended a refresher course approved by the Council within the preceding **three** years of signing any authorisation.

5.3 Applicants and Authorising Officers must have regard to this policy, the Codes of Practice listed at appendix 1, the latest guidance issued by the relevant statutory Commissioners and any other statutory Codes of Practice (e.g. The Regulators Code) when making their applications or determinations.

6. General Rules on Authorisations

6.1 Since 1st November 2012 authorisations for Directed Surveillance by Local Authorities may only be granted:

6.1.1 For the purpose of preventing or detecting conduct which constitutes one or more criminal offences; **AND**

6.1.2 That offence is punishable, whether on summary conviction or on indictment, by a maximum term of at least 6 months of imprisonment; **OR**

6.1.3 The offence relates to the sale of alcohol, tobacco or relevant nicotine inhaling products (e.g. e-cigarettes) to persons under the age of 18.

This is known as the Imprisonable Crime Threshold.

6.2 **Necessity and Proportionality**: An authorisation should not be granted unless the Directed Surveillance or use of CHIS (the activity) is both necessary **AND** proportionate.

6.3 The activity by a local authority can only be considered to be necessary where it is for the purpose of preventing or detecting crime.

6.4 The person considering the application for authorisation must consider whether the activities are proportionate to what is sought to be achieved by carrying them out. This involves balancing the intrusiveness of the activity on the target and others who might be affected by it, against the need for the activity in operational terms.

6.5 The proposed activity will not be proportionate if:

6.5.1 The intrusiveness is excessive in relation to the value of the information to be obtained; or

6.5.2 The information sought could be obtained by less intrusive means.

6.6 The following elements of proportionality must therefore be considered:

6.6.1 Balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;

6.6.2 Explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;

6.6.3 Whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;

6.6.4 Evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

6.7 **Collateral Intrusion** refers to the intrusion into the privacy of persons other than those who are the subject of the investigation.

6.8 Measures should be taken to minimise both the risk and the extent of such intrusion. An application for authorisation should consider the risk of such intrusion and the Authorising Officer must take such risk into account in reaching a judgement as to whether or not the proposed directed surveillance/use of covert human intelligence source is proportionate.

6.9 If the investigation unexpectedly interferes with the privacy of persons who are not covered by the authorisation, the Authorised Officer must be informed without delay.

7. Management of Covert Human Intelligence Sources

7.1 An Authorising Officer should not grant an authorisation for use of a CHIS unless they are satisfied of the following:

7.1.1 At all times there will be an officer (Handler) with day-to-day responsibility for dealing with the CHIS on behalf of the Council and for the source's security and welfare;

7.1.2 At all times there will be an officer (Controller) within the Council who will have responsibility for the management and supervision of the Handler and general oversight of the use made of the CHIS;

7.1.3 At all times there will be an officer responsible for maintaining a record of the use made of the CHIS and other matters as may be specified by regulation; and

7.1.4 Records maintained by the Council that disclose the identity of the CHIS will not be available to persons except to the extent that there is a need for access to them to be made available to those persons.

7.2 The Authorising Officer should not be involved in the management of any investigation involving the use of a CHIS. Neither should they act as Controller or as Handler for an authorisation approved by them. These roles should not be carried out by the same person.

7.3 The safety and welfare of the CHIS and foreseeable consequences to others should be taken into account in deciding whether or not to grant an authorisation.

7.4 A risk assessment determining the risk to the CHIS in acting as a source of information to the Council, and in particular identifying and assessing the risks should the identity of the CHIS become known, should be carried out. The welfare and security of the CHIS after the operations has ceased should be considered at the outset.

7.5 The Handler should report to the Controller any concerns about the personal circumstances of the CHIS, insofar as they might affect;

- the validity of the risk assessment
- the conduct of the CHIS, and
- the safety and welfare of the CHIS.

7.6 If appropriate such concerns should be reported to the Authorising Officer who will need to determine whether or not to allow the authorisation to continue.

8. Who can Grant an Authorisation?

8.1 The law permits authorisations for directed surveillance and use of a CHIS to be granted by a Director, Head of Service, Service Manager or equivalent.

8.2 Where it is likely that confidential information may be obtained or a CHIS is to be deployed who is either a vulnerable individual or a juvenile, the activity must be authorised by the Head of Paid Service or (in their absence) the person acting as the Head of Paid Service.

8.3 Any application for an authorisation must be made to an Officer authorised by the Council and listed in Appendix 3 as "Authorising Officers". Officers should not normally authorise investigations in which they are directly involved. All Authorising Officers must have received relevant training.

8.4 Intrusive surveillance cannot be undertaken by local authorities. Officers CANNOT therefore authorise intrusive surveillance.

8.5 If there is any difficulty in assessing whether an application is necessary or appropriate, contact the Head of Legal Services.

9. Obtaining an Authorisation – General

9.1 An authorisation must be given in writing; the exception in relation to urgent cases permitting oral authorisation is not available to a Local Authority.

9.2 The Officer seeking an authorisation (Applicant) should apply through their own line management structure unless it is impracticable in the circumstances (e.g.

because no Authorising Officer in the relevant service is available or the Authorising Officer is, or has been, involved in the investigation.

9.3 It is acknowledged that both Public Protection and Legal Services have the greatest level of awareness of the authorisation process (due to the very nature of their operations) and the Council will signpost colleagues from other service areas to those with familiarity to ensure that the policy is followed.

9.4 An application for authorisation should be made on the relevant form listed at Appendix 4. Both the Applicant and the Authorising Officer shall have regard to any guidance issued on the use of those forms.

9.5 Please refer to the general authorisation flowchart set out in Appendix 5 and the notes thereto. The detailed process is set out below by reference to Appendix 6. This information is very important to protecting the integrity of the process.

9.6 Authorising Officers must not consider an application that has not been registered with, and contains the URN assigned by, Legal Services.

9.7 Authorising Officers must state explicitly what conduct is being authorised (refer to s28(4) of RIPA). That is the "*who, what, where, when and how"* in relation to what is being authorised. They should avoid repetition or simple reference to what has been requested in the application.

9.8 Authorising officers must direct their mind to each of the relevant tests and satisfy themselves on matters such as proportionality and necessity. As noted above, any activity authorised should be the least intrusive option for securing the necessary information.

9.9 It is helpful, particularly in relation to a CHIS, to explain in the application the intended use and conduct of the CHIS using descriptive language about the specific activities that are being authorised and the reason why. The Code of Practice gives examples of how this could be applied.

9.10 Authorising officers must fully appreciate the capability of any surveillance equipment intended to be used together with an understanding of where and how it is to be deployed as a consequence of their authorisation.

10. Service Equipment

10.1 Where specific equipment is purchased to be used for surveillance purposes and is maintained by the Service for that purpose it will feature on a register. This register will list the full technical specification and capabilities of that equipment and may be referred to in the request by both the applicant and the authorising officer.

10.2 A copy of each Service Equipment Register will be held by the Senior Responsible Officer of the Council.

10.3 Standard ICT equipment which is issued by the Council to Officers such as lap tops or smart phones must never be used to undertake covert surveillance.

11. CCTV

11.1 Because CCTV is usually overt (i.e. members of the public are made aware that a CCTV system is in operation) an authorisation is not normally required for the use of CCTV equipment. However, there may be occasions when a covert CCTV system is used for the purposes of a specific investigation or operation in which case an application for directed surveillance may be required. Specialist advice from the Head of Legal Services should be sought in such circumstances.

11.2 The use of body worn video and/or audio recording equipment by Officers will normally be carried out overtly, they should comply with the requirements of the Surveillance Camera Code of Practice[4] (2013 CoP). Where such equipment is to be used covertly, this policy will apply.

11.3 If any Service considers the use of body worn video and/or audio recording equipment advice should be sought from Legal Services after consideration of the guiding principles mentioned in the 2013 CoP.

12. Underage Sales and Test Purchase Operations

12.1 By their nature all test purchase operations are covert and conducted for a specific operation. When planning test purchase activities the Officer in Charge (OiC) of the specific operation must consider the application of RIPA, with regard to both Direct Surveillance and CHIS.

12.2 The Assistant Surveillance Commissioners report of 2015 made a number of observations with regard to the application of RIPA to such operations, including;

12.2.1 The IPCO Procedures and Guidance of 2014 (previously issued by the OSC) make reference to the desirability of obtaining authorisation where covert recording equipment or an observing officer are deployed (repeated at point 244 in the procedures and Guidance of 2016);

12.2.2 The BRDO Code emphasises the Chief Surveillance Commissioners' guidance on this aspect of operations;

12.2.3 The introduction of the 'Imprisonable Crime Test' clearly indicates the governments view that authorisation is appropriate.

12.3 Test purchase operations relating to alcohol are considered within the relevant RIPA Codes of Practice at Appendix 1. These indicate that where a juvenile has been employed other than as a CHIS, and either covert equipment is used or an adult is observing, a Direct Surveillance authorisation must be considered.

12.4 The need for a Directed Surveillance authorisation will be determined by whether it is likely that private information will be obtained about a person. The OiC must have regard to this policy above when considering this.

12.5 Where there is to be any prolonged surveillance or repeated attempts at the same premises, an authorisation for a CHIS must also be considered. Officers

[4] Home Office: Surveillance Camera Code of Practice; June 2013 https://www.gov.uk/government/publications/surveillance-camera-code-of-practice

should note that where a CHIS is used, the meaning of "information" is not restricted to private information[5].

12.6 Where the OiC does not apply for an authorisation for either Directed Surveillance or the use of a CHIS, their rationale must be recorded and retained on file for a period of three years. These records will be subject to review by the Monitoring Officer and will be available for examination by IPCO.

13. Third Party Authorisations

13.1 On occasion Officers of the Council may work together with other agencies for the purpose of preventing or detecting crime. Where such work would require an authorisation under this policy, the other agency may take responsibility for obtaining that authorisation through its own procedure. That agency will be responsible for the recording and retention of the Authorisation in accordance with the Act.

13.2 The Line Manager of any West Berkshire Officer required to engage in third party authorised activity must obtain a copy of the authorisation to ensure that Officers are:

13.2.1 Properly authorised;

13.2.2 Acting at all times within the terms of that authorisation; and

13.2.3 Acting at all times within the parameters of the operating procedures of West Berkshire District Council.

13.3 That Line Manager will be responsible for passing details of the authorisation to Legal Services in accordance with the process at Appendix 6. This also includes the completion of review meetings, cancellations and any revocation decisions.

14. Social Network Sites (SNS) – Online Investigations

14.1 The Surveillance Commissioner has made a series of comments about local authorities accessing information available on the internet. There was concern expressed that they were doing this without direction, oversight or regulation and reiterated the view that certain activities would require authorisation.

14.2 These concerns were raised again in the report of 2016[6] and a letter was sent to all local authorities to highlight the matter. The OSC Procedures and Guidance July 2016 (now under IPCO), point 289, Covert Surveillance of Social Networking Sites, is reproduced at Appendix 6.12.

14.3 The use of the internet to gather information to profile targets prior to and/or during an operation may be considered Directed Surveillance. The risk of Collateral Intrusion is also likely to be an issue and must be fully considered as part of any assessment of the application of RIPA prior to the activity taking place.

[5] RIPA s. 26(8)

[6] *Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to the Scottish Ministers 2016 -2017, https://www.ipco.org.uk/docs/OSC%20Annual%20Report%202016-17.pdf*

14.4 All Officers proposing to access social media must be familiar with the relevant codes of practice and guidance listed at Appendix 1. They should have particular regard to paragraphs 3.10 to 3.17 of the Code relating to Directed Surveillance and paragraph 4.11 to 4.17 of the Code relating to the use of a CHIS when considering the application of RIPA.

14.5 Where the activity is likely to require an ongoing, covert, relationship with other SNS users, this may come within the parameters of a CHIS. Where such activities are contemplated but no authorisation is sought, the Officer in Charge must record their reason and retain this in compliance with the policy.

14.6 On-line investigations shall only be conducted on equipment designated for that purpose. Such equipment will not be attached to the Council's network. Officers must not use personal accounts for accessing social media as part of their enquiries.

14.7 Only Officers who have attended suitable training will be authorised to conduct on-line investigations under a RIPA authorisation.

14.8 Officers must be familiar with, and have regard to, the Council's policy on the use of Social Media; section 13 of the Code of Conduct for Staff[7].

14.9 Officers must comply with the requirements of Appendix 8 which specifies the Investigatory Use of Social Network Sites.

15. Roles and Responsibilities

15.1 Senior Responsible Officer (SRO)

The Codes of Practice consider it good practice for a Senior Responsible Officer to be appointed and made responsible for the following:

15.1.1 The integrity of the process in place within the Council;

15.1.2 The management of covert human intelligence sources (CHIS);

15.1.3 Compliance with Part II of RIPA and with the Codes of Practice;

15.1.4 Oversight of the reporting of errors to the relevant oversight Commissioner and the identification of the causes of errors and the implementation of processes to minimise repetition of errors;

15.1.5 Engagement with the IPCO inspectors when they conduct their inspections;

15.1.6 Where necessary, oversight of the implementation of post inspection action plans approved by the relevant oversight Commissioner.

15.2 Heads of Service

15.2.1 In supporting the SRO, Heads of Service should ensure that the communicaitons related to the policy are effective and comprehensive.

[7] *Code of Conduct of Staff http://intranet/CHttpHandler.ashx?id=15446*

This is to minimise the risk of unauthorised activity and to improve awareness across the Council.

15.2.2 Head of Public Protection and Culture will ensure that the Joint Public Protection Committee is aware of the policy and advise on its application.

16. Oversight of RIPA and its Use

16.1 Elected members of the Council have an overview and scrutiny role in relation to the use of RIPA by its officers. The SRO will provide regular reports to designated members and facilitate an annual review of the use of RIPA to ensure it is in compliance with this policy and that the policy remains fit for purpose.

17. Implementation of the Policy

17.1 This Policy will be supported and implemented by the development and publication of standard documentation as listed in the Appendices. These documents may vary between different service areas but will be the responsibility of the relevant Head of Service to update in line with this policy.

18. Failure to comply with the Council's RIPA Policy

18.1 This document provides staff and others with essential information regarding RIPA and sets out conditions to be followed. It is the responsibility of all to whom this Policy document applies to adhere to these conditions. Failure to do so may result in:

- Withdrawal of access to relevant services;
- Informal disciplinary processes;
- Formal disciplinary action (in accordance with the relevant HR policies and procedures).

18.2 Additionally if, after internal investigation, a criminal offence is suspected, the Council may contact the police or other appropriate enforcement authority to investigate whether a criminal offence has been committed.

19. Review

19.1 This policy will be reviewed to respond to any changes and at least every 3 years.

19.2 The Service responsible for reviewing and maintaining this Policy is Public Protection and Culture in consultation with Legal Services.

Appendices

1. **APPENDIX 1 - RIPA Codes of Practice**

1.1 COVERT SURVEILLANCE AND PROPERTY INTERFERENCE.

1.2 COVERT HUMAN INTELLIGENCE SOURCES.

1.3 ACQUISITION, DISCLOSURE AND RETENTION OF COMMUNICATIONS DATA.

Above codes can be found on the Home Office web site under RIPA Codes;(www.gov.uk/government/collections/ripa-codes)

2. **APPENDIX 2 - RIPA Guidance**

2.1 ACQUISITION AND DISCLOSURE OF COMMUNICATIONS DATA.

Guidance for applicants and designated person considering necessity and proportionality. (**www.gov.uk/government/publications/guidance-notes-for-chapter-ii-application**)

2.2 Home Office guidance to local authorities in England and Wales on the judicial approval process for RIPA and the crime threshold for directed surveillance. **(www.gov.uk/surveillance-and-counter-terrorism)**

2.3 IPCO Procedures and Guidance (and previously issued by OSC).

Oversight arrangements for covert surveillance and property interference conducted by public authorities and to the activities of relevant sources (Available at **www.ipco.org.uk**).

3. APPENDIX 3 - Authorised Officers Under RIPA

1. **Name**	**2. Title**	**3. Service Area**	**4. Enhanced Authorisation**
Nick Carter	Chief Executive	Head of Paid Service	Confidential Information Vulnerable Individual & Juvenile sources
MONITORING OFFICER AND SENIOR RESPONSIBLE OFFICER			
Sarah Clarke	Head of Legal Services	Legal Services	
AUTHORISING OFFICER AND DESIGNATED PERSON			
Paul Anstey	Head of Public Protection & Culture	Building Control, Emergency Planning, Energy Management, Heritage, Libraries, Museum, Public Protection, Sport and Leisure.	
AUTHORISING OFFICER			
Sean Murphy	Public Protection Partnership Manager	Building Control, Environmental Health, Licensing & Trading Standards	

4. APPENDIX 4 - Authorisation and Other Forms

4.1 Home Office Issue

4.1.1 Authorisation Directed Surveillance

4.1.2 Review of a Directed Surveillance Authorisation

4.1.3 Renewal of a Directed Surveillance Authorisation

4.1.4 Cancellation of a Directed Surveillance Authorisation

4.1.5 Application for the use of Covert Human Intelligence Sources

4.1.6 Reviewing the use of Covert Human Intelligence Sources

4.1.7 Renewal of authorisation to use Covert Human Intelligence Sources

4.1.8 Cancellation of Covert Human Intelligence Sources

All current forms can be found on the Home Office web site by searching for "RIPA Forms" As at December 2018 they can be found here:
https://www.gov.uk/government/collections/ripa-forms--2

4.2 Internal Forms

4.2.1 RIPA/CR1 – Initial Notification to Legal Services

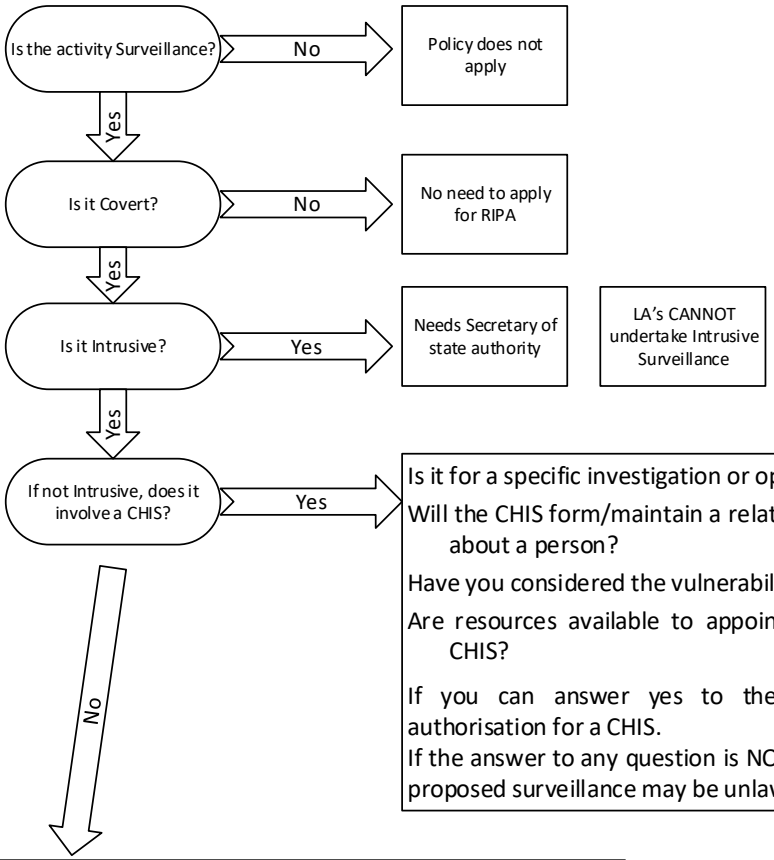
4.2.2 RIPA/CR2 – Notification of approval by Authorising Officer

4.2.3 RIPA/JA – Application for Judicial Approval, parts A and B

4.2.4 RIPA/JA1 – Application refused on Judicial Review - internal remedy

4.2.5 RIPA/JA2 – Application refused and quashed on Judicial Review – legal challenge considered

5. APPENDIX 5 - Authorisation Process – General and Flowchart



Is it:

For the purposes of a specific investigation or operation?

Likely to result in obtaining private information about any person?

A Foreseen/planned response

If the answer to all 3 questions is YES, apply for authorisation for DIRECTED SURVEILLANCE

If the answer to any question is NO, RIPA protection does not attach and the proposed surveillance may be unlawful

POINTS TO CONSIDER BY AUTHORISING OFFICERS

1. Is the authorisation:

- **Necessary for detection or prevention of crime?**
- **Proportionate to what it seeks to achieve?**
- **Proportionate to the intrusion of privacy including collateral intrusion?**

2. Is the operation likely to result in obtaining Confidential Information?

- **If yes refer to Chapter 4 of the appropriate Code of Practice listed at appendix 1**

3. In the case of a CHIS

- **Ensure an appropriately trained Handler and a Controller have been appointed and arrangements are in place to manage the source.**
- **That a Risk Assessment is carried out.**
- **Consider the Vulnerability of individuals and whether or not Juveniles involved.**
- **Has the Secretary of State issued any Order [S29(7)] regarding a CHIS.**

6. APPENDIX 6 - Authorisation Process – Detail and Flowchart

6.1 Introduction

6.1.1 This process sets out how applications must be processed and should be read in conjunction with the West Berkshire Council (the Council) policy for undertaking activities under the Regulation of Investigatory Powers Act (the Act).

6.1.2 Under the provision of RIPA the Council is required to maintain a Central Register (the Register) of all applications and subsequent activity for authorisation under the Act. This Register will be held by Legal Services (LS) on behalf of the Council.

6.1.3 Applications shall be made on the forms indicated at Appendix 4 of the Council RIPA policy. The internal forms listed can be found on the intranet here.

6.2 Application

6.2.1 When an Officer (the Applicant) wishes to make an application under RIPA they must first obtain the agreement of their line manager or other senior officer, but not an Authorising Officer (AO). This agreement must be recorded on the appropriate Service investigation record. Once agreed, the Applicant will register their intent with LS by completing form RIPA/CR1 and sending it electronically to them via the following generic email account; ripa@westberks.gov.uk.

6.2.2 On receipt of the form LS will undertake the following actions:

- Assign a unique reference number (URN) to the application;
- Enter the detail from the form on to the Register; and
- E-mail the URN to the applicant.

6.2.3 The Applicant will enter this URN on all pages of the application and submit this in the normal way to an AO for consideration. Applications without the URN will be refused.

6.2.4 Applications should not be passed to an AO for an 'informal review' prior to the formal application process being commenced.

6.3 Consideration by AO

6.3.1 The AO will either refuse or approve the application. The application may be approved with modifications or restrictions on the activity requested.

6.4 Application Refused

6.4.1 The AO will inform the applicant of their reasons and send the completed application form to LS who will update the central register and retain the application in accordance with Council policy.

6.4.2 Where an application is refused because the AO indicates further detail is required, the Applicant may submit a new application. This second application must be registered with LS by following the process at paragraph 2 above and should be linked to the initial application by reference to the original URN.

6.5 Application Approved

6.5.1 The AO will pass the completed form to the Applicant, drawing their attention to any modifications/restrictions they have placed on the activity.

6.5.2 The AO will complete form RIPA/CR2 and pass this to LS via the generic email account.

6.6 Judicial Approval

6.6.1 The Applicant is responsible for liaising with the Magistrates' Court office to ensure the approved authorisation is put before a Justice of the Peace (JP) without delay.

6.6.2 They will complete the Application for Judicial Approval form, (RIPA/JA), and submit this together with the original RIPA application and supporting documentation, in person before a JP.

6.6.3 The JP will consider the application and make an Order in respect of it, completing part B of the Application for Judicial Approval form.

6.7 Authorisation Approved

6.7.1 The Applicant will pass the completed RIPA application, associated paperwork and Order to LS within ONE working day.

6.7.2 Copies should be retained for the investigation file. These documents must be available for the briefing of officers involved in the authorised activity.

6.7.3 LS will update the Register and set reminders to the AO for renewal and review dates as indicated on the application.

6.8 Authorisation Refused

6.8.1 When an application is refused the Order will be passed to LS within one working day. A copy shall be passed to the AO, together with the refused RIPA application, within one working day.

6.8.2 The reasons for refusal shall be considered by the AO who will consider:

a) if the application can be enhanced to address the reasons for refusal;
b) if a new application should be submitted;
c) to cancel the application - alternative measures to RIPA should be considered; or

d) whether the decision to refuse the application was, in their opinion, wrong in law.

6.8.3 Where (a) applies:

- This will only be applicable if the text of the original RIPA application remains unaltered through the review and reapplication process. The appropriate measures will be identified by the AO and recorded on Part A of form RIPA/JA1. This form, together with the RIPA application will be passed back to the applicant for action.

- A copy of form RIPA/JA1 will be sent to LS by use of the generic email address.

- LS will update the Register.

- Once actioned the applicant will complete Part B of form RIPA/JA1 and submit this together with the original application and supporting information to the AO.

- The AO will review the information and once satisfied with the information will complete part C of the RIPA/JA1. The completed paperwork will be passed to the applicant who will follow the procedure at point 6.

6.8.4 Where (b) applies:

- The AO will inform the applicant of his decision, complete part A of form RIPA/JA1 and send this together with the Order, original application and supporting paperwork to LS who will update the Register.

- The applicant will follow the process for a new application as at point 2 above. The new application must be linked to the refused application by reference to the URN of the first application.

6.8.5 Where (c) applies:

- The AO will inform the applicant of his decision, complete part A of form RIPA/JA1 and send this together with the Order, original application and supporting paperwork to LS who will update the Register.

- The applicant must, in consultation with their line manager, consider alternative operational methods to achieve the objective.

6.8.6 Where (d) applies:

- The AO will inform the applicant of his opinion, complete part A of form RIPA/JA2 and pass this together with the Order, original application and supporting paperwork to LS who will update the Register.

- The Head of Legal will asses whether a legal challenge should be made to the Order. His decision will be recorded on part B of form RIPA/JA2 and retained in accordance with the Policy. LS will be responsible for updating the Register with this decision.

- The AO and Applicant will be advised of the decision.

6.9 Authorisation refused and quashed

6.9.1 When an application is refused and quashed the Order will be passed to LS within one working day. A copy shall be passed to the AO, together with the refused application, within one working day.

6.9.2 The Order shall be considered by the AO who will complete part A of form RIPA/JA2 and pass this together with the Order, original application and supporting paperwork to LS who will update the Register.

6.9.3 The Head of Legal will determine whether a legal challenge should be made to the Order. His decision will be recorded on part B of form RIPA/JA2 and retained in accordance with the Policy. The Register will be updated with this decision and the Authorising Officer advised via email.

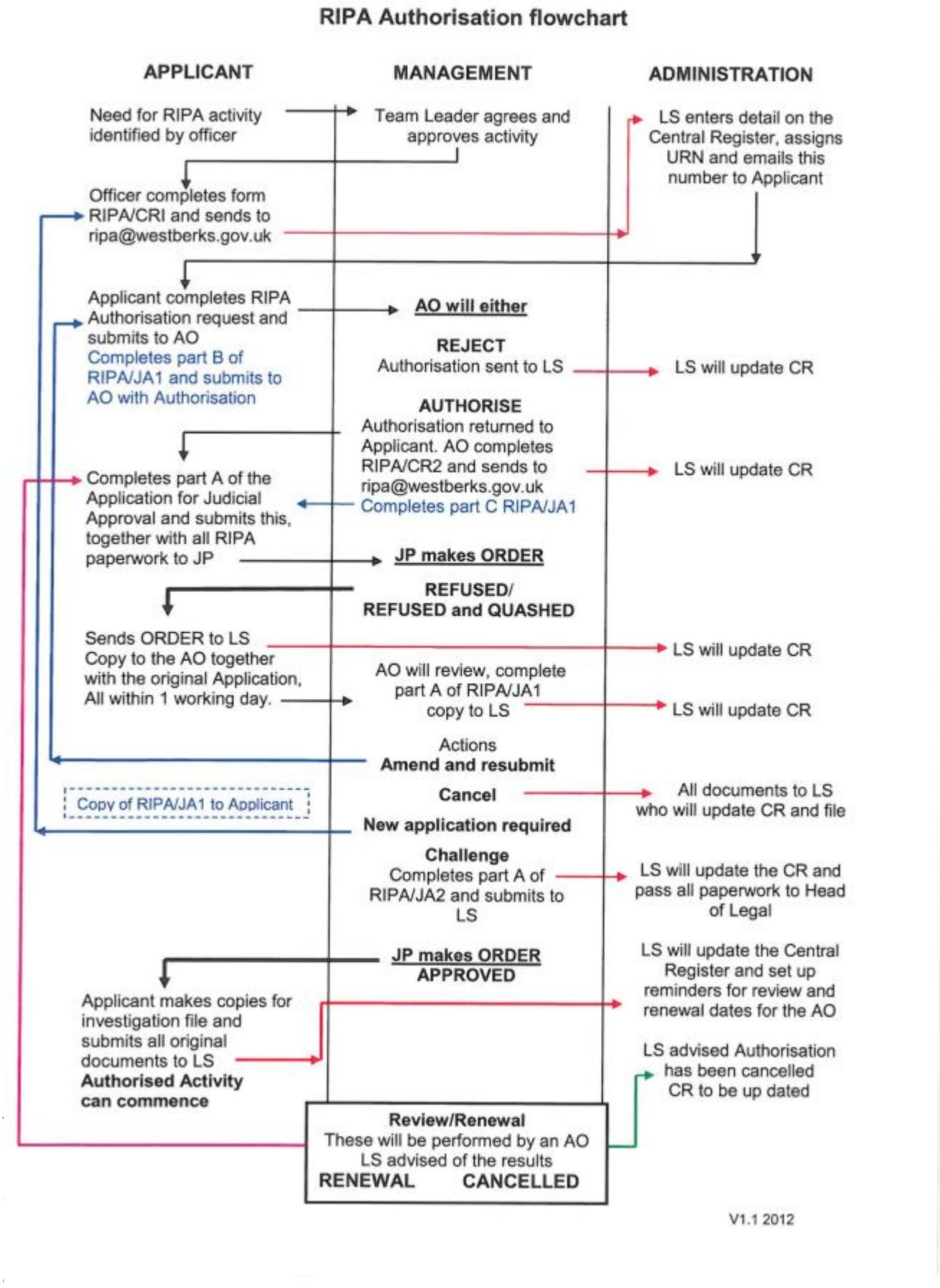
6.10 Third Party Authorisations

6.10.1 Where officers of the Council are authorised for surveillance activities by another agency a copy of the Authorisation must be passed to LS for recording on the Central Register before the activity commences.

6.10.2 An Officer of the Council must be identified as Lead Investigator with responsibility for ensuring all officers of this Council act in accordance with the specific Authorisation and all other legal requirements.

6.10.3 All activities undertaken by officers of the Council as part of the Authorisation will be recorded and reported by the Service as if the Authorisation was granted to the Council.

6.11 FLOW CHART



are applied. In some cases data may be deemed private communication still in transmission (instant messages for example). Where privacy settings are available but not applied the data may be considered open source and an authorisation is not usually required. Repeat viewing of "open source" sites may constitute directed surveillance on a case by case basis and this should be borne in mind.

289.2 Providing there is no warrant authorising interception in accordance with section 48(4) of the 2000 Act, if it is necessary and proportionate for a public authority to breach covertly access controls, the minimum requirement is an authorisation for directed surveillance. An authorisation for the use and conduct of a CHIS is necessary if a relationship is established or maintained by a member of a public authority or by a person acting on its behalf (i.e. the activity is more than mere reading of the site's content).

289.3 It is not unlawful for a member of a public authority to set up a false identity but it is inadvisable for a member of a public authority to do so for a covert purpose without an authorisation for directed surveillance when private information is likely to be obtained. The SRO should be satisfied that there is a process in place to ensure compliance with the legislation. Using photographs of other persons without their permission to support the false identity infringes other laws.

289.4 A member of a public authority should not adopt the identity of a person known, or likely to be known, to the subject of interest or users of the site without authorisation, and without the consent of the person whose identity is used, and without considering the protection of that person. The consent must be explicit (i.e. the person from whom consent is sought must agree (preferably in writing) what is and is not to be done).'

8. APPENDIX 8 - Investigatory Use of Social Network Sites (SNS)

8.1 Introduction

This document sets out how Services within West Berkshire Council (the Council) will use social network sites and should be read in conjunction with other relevant policies including;

- ICT Policy and User Usage Agreement
- Security Policy
- Code of Conduct of Staff

8.2 Purposes for using SNS

Services will access SNS in different ways:

8.2.1 Open and overt exchange of information with users;

8.2.2 Viewing information about users which is openly available, without any need to log in to the SNS, in order to verify information. This may be done overtly or covertly; and

8.2.3 Covertly viewing information and/or engaging with a user to obtain information about them, another person or a business.

These are explained in more detail below.

The purposes for which Services may wish to access SNS will include but is not limited to the following and it will be for the officer to determine which of the methods of accessing the SNS is appropriate according to the circumstances:

- Monitoring activities of licensed premises with regard to irresponsible drink promotions.
- Monitoring the promotion of bands that are known to have caused complaints relating to noise levels.
- Viewing personal areas to verify the details provided by a benefit claimant (living alone, fitness to work, etc)
- Checking residency with regard to school catchments areas
- Gathering information which may later become intelligence used to direct resources.
- Obtaining any information which provides evidence of a prima facia offence.

8.3 Open and overt exchange of information with users

For the purpose of this document 'overt use' is defined as the use of a SNS by Services in an open manner with the intent of sharing information with individual stakeholders or groups of stakeholders.

Those individuals or groups will be aware of our presence on their area (wall, space, page, etc) of the SNS. This will include areas used by businesses for advertising their products or services (e.g. the 'fan' section on Face Book). Where information is obtained from such areas which may lead to any form of enforcement action, this information must be handled in accordance with paragraph 6 of this document.

When employees of a Service are engaging openly with a business or individual as a representative of the Council they will operate in accordance with the policy. Services should set up corporate accounts which do not supply private information about individual employees. Access will normally be via networked computers which are operated and maintained in accordance with the Council's policies.

SNS access in this manner will not require Regulation of Investigatory Powers Act (RIPA) authorisation. Officers must still act in accordance with the investigation policies and procedures relevant to their Service as well as the requirements of this document.

Access will be monitored in accordance with the Policy and other relevant corporate strategies.

8.4 Viewing information about users which is openly available

Although users will not be aware of activity undertaken by Officers in viewing their SNS pages, subject to the considerations referred to below, this may not classed as covert surveillance for the purpose of RIPA.

There is unlikely to be a reasonable expectation of privacy by the user who has published this information about themselves and made it freely available for anyone to view.

Information that is considered as being openly accessible is only that which is capable of being accessed without logging on to the SNS as a user. If you need to log on to an SNS to access information about a person, that must be done either overtly or in accordance with the requirements for the covert acquisition of information.

Consideration should be given to the means of recording the information viewed and by what method. This information would also be required in order to comply with the provisions of the Criminal Procedure and Investigations Act 1996 (CPIA) where applicable.

Investigators should refer to their Service procedure notes for the method of doing this. Officers must still act in accordance with the investigation policies and procedures relevant to their Service as well as the requirements of this document.

Notwithstanding the above, those viewing information that is freely and openly available on an SNS must always consider in each case whether the user who's SNS is being viewed;

- might reasonably be aware of just how much of their personal information is openly accessible,
- and whether the SNS user might have inadvertently given public access to certain information.

This is not an easy task as it involves trying to guess what the SNS user was thinking. The more intimate or sensitive the personal information is likely to be, the greater the caution that should be exercised in viewing and recording the information. You may be required to demonstrate proportionality and necessity in relation to the user's Article 8 rights and in determine whether such information can properly be used in relation to the matter being investigated.

In circumstances where officers are considering accessing SNS for the purpose of obtaining information which is not required for a criminal investigation, the activity being contemplated would fall outside the scope of RIPA. However, in order to ensure that proper regard has been had to the Article 8 rights of the individual, consideration should be given to completing a "Consideration of RIPA to Directed Surveillance activities" form.

Before accessing SNS on any occasion, officers must first have regard to sections 3.10-3.17 of the Covert Surveillance and Property Interference Code of Practice.

8.5 Covertly engaging with a user to obtain information

For the purpose of this document covert use is defined as the use of SNS by Services to gather information to direct their activities in relation to the prevention and detection of crime, the apprehension or prosecution of offenders or to take any other action in respect

of a regulatory breach, except where that information is being obtained either by open and overt interaction with the user or where the information is openly available.

Before accessing an SNS covertly the investigating officer must give consideration to the provisions of RIPA. It is possible that the activity may be classified as Directed Surveillance or that the accessing officer may be acting as a Covert Human Intelligence Source (CHIS). The application for access will record those considerations along with the conclusion. Where it is determined that no RIPA application is required the appropriate paperwork on the case file will be endorsed to that effect by the appropriate officer or manager. If a RIPA authorisation is required then the Councils RIPA procedures together with any complementary Service policy for that process will be followed and access not granted until such time as the activity has been properly authorised in accordance with the legal process.

Where an officer wishes to access an SNS with the intent of gathering information about a business or individual (target) without the knowledge of that target, they will deemed to be acting covertly for the purpose of this document. Covert access will always be considered as an investigation and all officers must act in accordance with the investigation policies and procedures relevant to their Service as well as the requirements of this document.

For covert operations an anonymous user account will be set up which can not be traced back to the Service or any individual employed by the Council. These accounts will be maintained by the individual Service who will put in place processes for controlling and monitoring the access and use of the accounts.

Officers must have regard to sections 4.11-4.17 of the CHIS Code of Practice which provides useful guidance and context regarding online covert activity. Where there is any doubt, advice should be sought from the Senior Responsible Officer.

Access will be monitored in accordance with the Policy and other relevant corporate strategies.

8.6 Human Rights and Data Protection Act considerations

During an investigation an important consideration is the right of respect for private and family life (Article 8) and any interference with this right must be lawful, necessary and proportionate. Whilst RIPA provides a framework that enables specific types of interference with this right e.g. for covert surveillance to be lawful, the Human Rights aspects must always be considered even where RIPA is not engaged.

When viewing SNS as described above, officers must consider whether the information that has been published on an SNS attracts any reasonable expectation of privacy. Guidance suggests that if any expectation of privacy is claimed it is unlikely to be reasonable given the various warnings that are usually contained on the SNS privacy policies.

Interference with any privacy right claimed will require a legal basis, which for investigations undertaken by the local authority will be found in the relevant legislation e.g. Health and Safety at Work Act or trading standards legislation. The carrying out of investigatory work that does not trigger the application of RIPA remains a lawful interference with any right of respect to private and family life, provided activity is both necessary and proportionate.

Any personal information that is collected from viewing SNS must be held and processed in accordance with the Data Protection Act, as well as any investigation and evidential protocols that are in place.

8.7 Authorisation

All access to SNSs must be authorised in advance by an appropriate Team Leader/Manager in accordance with the Policy. This authorisation is in addition to any authorisation that might be required under RIPA and it does not detract from the responsibility to keep appropriate records of the SNS access and the information viewed and used.

8.8 Equipment

Officers must not under any circumstances use their personal IT equipment or any other IT equipment that is not provided by the Council for undertaking any of the activities to which this document relates.

The Service should provide dedicated standalone computers for covert internet activity. Networked computers must not be used for this type of exercise. Printed information obtained from networked computers will not normally be sufficient for evidential purposes and officers should only resort to using these where there is no other means available to them.

SNS information is primarily transmitted and stored in a digital format and it is important that this is captured in such a way that the integrity of the information is not compromised. There are a number of published guides that are relevant to the capture, storage and production in court of computer based evidence. All officers charged with the production of computer based evidence which may result in legal proceedings should be familiar with these documents.[8]

8.9 Criminal Procedures and Investigations Act 1996 (CPIA)

Where officers acquire information which may result in regulatory action they must ensure they secure this information in such a way that the Service can discharges its duties under the CPIA in any future proceedings. Regulatory action includes, but is not restricted to, the following:

- Prosecution, Simple Caution, Administrative Penalties, Written or Verbal warnings relating to criminal breaches
- Issuing of Fixed Penalty Notices, Penalty Notice for Disorder or other statutory fines
- Suspension or review of any benefits
- Review of any licences issued by the Authority
- Use of Civil sanctions to prevent future breaches of legislation

[8] Storage, Replay and Disposal of Digital Evidential Images, Home Office Publication 53/07
Digital Imaging Procedure v2.0 November 2007, Home Office Publication 58/07
Good Practice Guide for Computer-Based Electronic Evidence, ACPO 2007

8.10 Personal use

The Code of Conduct of Staff policy sets out the standards expected of employees of the Council in their personal use of Social Network Sites. Employees should ensure that in their personal use of SNS they do not provide details about their employment that might compromise their health & safety. This is particularly relevant where they are engaged in enforcement activities in their routine work.