GUILDFORD BOROUGH

# Covert Surveillance Policy
## and Procedure Note

**DOCUMENT INFORMATION**

| | |
|---|---|
| Origination/author: | Ciaran Ward Information Rights Officer |
| Version: | 2018:1 |
| This document replaces: | Covert Surveillance Policy 2015-1 |
| Approved by: | |
| Date of approval: | |
| Last reviewed: | N/A |
| Next review date: | March 2020 |
| Target Audience: | All staff |
| Method of communication: | NETconsent (Targeted mailing list) |

## Contents

**Part 1: Policy**
1. Background and summary
2. Policy Statement
3. Scope of this policy and procedural document
4. Review of this policy and procedural document
5. Governance roles, responsibilities and communications
6. Complaints

**Part 2: Procedures**
7. Summary of authorisation procedure

8. Authorisation of surveillance
    - 8.1. Activity requiring authorisation
    - 8.2. Unique reference numbers (URNs)
    - 8.3. Authorising Officers – roles and responsibilities
    - 8.4. Authorising the acquisition of Confidential Material
    - 8.5. Authorisation for the use of sources
    - 8.6. Authorising acquisition of communications data
    - 8.7. Communications Data - special procedure
    - 8.8. Applying for judicial approval
    - 8.9. Training
    - 8.10. Activities by other authorities
    - 8.11. Joint investigations (collaborative working)

9. The “necessary and proportionate” test
    - 9.1. Responsibility for the test
    - 9.2. “Necessary”
    - 9.3. “Proportionate”

10. Duration, reviews, renewals and cancellation of authorisations
    - 10.1. Duration
    - 10.2. Reviews
    - 10.3. Renewals
    - 10.4. Cancellations

11. The central record

12. Retention and destruction
12.1. Retention of material obtained through surveillance
12.2. Records maintained by the investigating officer
12.3. Covert Human Intelligence Source (CHIS) records

**Part 3: Appendixes**
Appendix A: Authorised Officers
Appendix B: Definitions
Appendix C: Further guidance on types of surveillance
Appendix D: Further examples to help you decide whether your activities are covered by this policy
Appendix E: Covert Human Intelligence Sources – using minors
Appendix F: List of approved forms

# PART 1 - POLICY

## 1. BACKGROUND AND SUMMARY

1.1. The Regulation of Investigatory Powers Act 2000 (RIPA) and associated legislation set out a regulatory framework for the use of covert investigatory techniques by public authorities. It does not provide any powers to carry out covert activities but regulates them in a manner that compatible with the Human Rights Act 1998, particularly Article 8 – the right to respect for private and family life ("Article 8 rights").

1.2. RIPA limits local authorities to using three covert investigation techniques, which are allowed only for the purpose of preventing or detecting crime or preventing disorder. The techniques are:

- directed surveillance – i.e. covert surveillance in places other than residential premises or private vehicles, where the investigation is likely to obtain information about any aspect of a person's private life or personal relationships with others, including family and professional or business relationships,

- covert human intelligence sources (CHIS) – this includes informants using a relationship with the individual under investigation or another person to obtain and pass on any information (not just private information). This can therefore include undercover officers, public informants and, in some circumstances, people who make test purchases,

- 'communications data' – specifically 'service use information' (such as the type of communication, time sent and its duration); and 'subscriber information' (which includes billing information such as name, address and bank details of the subscriber or telephone or internet services). **Note:** there is a third type of communications data, referred to as 'traffic data' (which includes information about where the communications are made or received) – *under no circumstances can the Council authorise the acquisition of traffic data under RIPA nor may the Council intercept the content of any person's communications*.

1.3. The use of the above techniques must be authorised internally by a designated authorising officer and then by a magistrate. Directed surveillance can only be used where (1) *necessary* to investigate a suspected crime or disorder with a maximum sentence of at least six months' imprisonment and (2) *proportionate* (balancing the seriousness of the intrusion into privacy against the seriousness of the offence and whether the information can be obtained by other means). Where unauthorised evidence-gathering activity interferes with the right to respect for private and family life, and where there is no other source of lawful authority for it, the consequence may be that the evidence has been gathered unlawfully. The courts may therefore disallow the evidence, a complaint of maladministration could be made to the Ombudsman or Investigatory Powers Tribunal, and the Council could be ordered to pay compensation.

1.4. The Council has provided this policy and procedural document to ensure that any covert surveillance activity undertaken by Council officers is necessary, proportionate, authorised and conducted legally. This will help ensure that any evidence gained during any operation is lawful and permissible in Court and meets the aims of the investigation.

1.5. All involved with covert investigations must comply with this document and any further guidance that may be issued from time to time, by the Senior Responsible Officer (SRO) in respect of the Council's compliance with RIPA and its associated legislation.

1.6. In addition to this policy and guidance, officers must take into account the Codes of Practice issued under RIPA (the Codes of Practice are at https://www.gov.uk/government/collections/ripa-codes).

## 2. POLICY STATEMENT

2.1. Guildford Borough Council may use covert surveillance to carry out certain statutory functions. In order to do this in a fair and lawful manner, and in accordance with Human Rights legislation, the Council is committed to complying with the Regulation of Investigatory Powers Act 2000 (RIPA) and its associated legislation. Therefore, directed surveillance will only take place if it is to prevent or detect a criminal offence punishable by a maximum custodial sentence of at least six months or relates to the underage sale of alcohol and tobacco and where it has been authorised by an appointed Authorising Officer and a magistrate.

2.2. Officers shall seek an authorisation where the directed surveillance, the use of a source or the obtaining of communications data is likely to interfere with a person's Article 8 rights to privacy by obtaining private information about a person (whether or not that person is the subject of the investigation or operation). Obtaining an authorisation will ensure that the action is carried out in accordance with law and subject to stringent safeguards against abuse.

2.3. Guildford Borough Council will comply with the Covert Surveillance Codes of Practice Pursuant to Section 71 of RIPA (the Code). All officers who carry out covert surveillance activity will be required to follow the procedures and guidance set out in this policy document.

2.4. The Council will provide training for all staff that are, or may become, involved with covert evidence-gathering operations, as identified by the relevant head of service. The Council will also monitor its own working practice on a regular basis.

2.5. This Council is subject to periodical inspections by the Investigatory Powers Commissioner's Office (IPCO) to ensure compliance with RIPA and to review the Council's policies, procedures, and individual authorisations. Further details about inspections can be found at https://www.ipco.org.uk/

2.6. There is a statutory complaints system, which is welcomed by the Council. The Investigatory Powers Tribunal deals with complaints from members of the public about the use of the powers by public authorities. The Tribunal is separate from the IPCO. The Council welcomes this external scrutiny. It expects its officers to co-operate fully with these statutory bodies and to bring forward any proposals for improvement that may follow on from an inspection report or a Tribunal hearing.

## 3. SCOPE OF THIS POLICY AND PROCEDURAL DOCUMENT

3.1. This policy and procedural document relates to the authorisations of directed surveillance, sources (CHIS) and acquisition of communications data.

3.2. An authorisation under RIPA will provide lawful authority for the investigating officer to carry out the investigation as described in the application form and in accordance with any further direction given by the authorising officer and the magistrate.

3.3. Some investigations may not relate to the Council's core functions, such as the monitoring of the Council's e-mails and internet usage. It is important to recognise the interplay and overlaps with the Council's Acceptable Use policies and guidance, the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 ("Lawful Business Practice Regulations") and the Data Protection Act 1998. Authorisations under RIPA should be made ***where relevant*** and they will only be relevant where the **criteria** listed on the authorisation forms are fully met.

3.4. In particular, RIPA is not relevant to the following activities:

(a) covert surveillance by way of an immediate response to events;
(b) covert surveillance as part of general observation activities at trouble 'hotspots' and routine patrols;
(c) covert surveillance that does not relate to core functions, which should be conducted under legislation other than RIPA;
(d) overt use of CCTV and ANPR systems, which are regulated by the Data Protection legislation and associated codes of practice (includes body-worn cameras)
(e) certain other specific situations

3.5. Where RIPA is not relevant, other empowering legislation will apply instead. In addition, the Data Protection Act 1998 is likely to regulate the use and obtaining of any evidence relating to any living individual. In these cases, the officer responsible must carry out a privacy impact assessment (PIA) and seek advice from the Information Rights Officer (IRO).

## 4. REVIEW OF THIS POLICY AND PROCEDURAL DOCUMENT

4.1. RIPA and this document are important for the effective and efficient operation of the Council's actions regarding surveillance. Therefore, the SRO will keep this document under review. Authorising Officers must bring any suggestions for continuous improvement of this document to the attention of the SRO at the earliest possible opportunity.

4.2. Officers will review the policy annually in consultation with councillors. The associated procedures will also be reviewed regularly to reflect changes in legislation and good practice.

## 5. GOVERNANCE ROLES, RESPONSIBILITIES AND COMMUNICATION

**Senior Responsible Officer (SRO)**

5.1. The Managing Director (TBC) is the Senior Responsible Officer (SRO). The SRO is responsible for:

- the integrity of the process in place for the management of sources and directed surveillance;
- compliance with Part 2 of RIPA and the associated Codes;
- oversight of the reporting of errors to the relevant oversight Commissioner and the identification of both the cause(s) of errors and the implementation of processes to minimise the repetition of errors;
- engagement with the IPCO inspectors when they conduct their inspections, where applicable; and
- where necessary, oversight of the implementation of post-inspection action plans approved by the relevant oversight Commissioner
- ensuring appropriate training is available for Authorising Officers and relevant staff.

**RIPA Coordinating Officer**

5.2. The IRO is the RIPA Coordinating Officer. The RIPA Coordinating Officer will:

(a) monitor and keep the central record of authorisations,
(b) provide day-to-day advice on the use of covert surveillance and
(c) will provide a quarterly report to the Corporate Governance Group and the Leader of the Council. This report will set out the number and nature of covert surveillance authorisations under RIPA, highlighting any areas of concern.
(d) provide governance support to the SRO as required or directed

**Single Point of Contact (SPoC) for communications data**

5.3. The Council will use the SPoC service provided by the National Anti-Fraud Network (NAFN), and the Investigations Manager or the Information Rights Officer are the designated contacts.

5.4. The SPoC:

a) where appropriate, assesses whether access to the communications data is reasonably practical for the postal or telecommunications operator;

b) advises applicants and Authorising Officers on the practicalities of accessing different types of communications data from different postal or telecommunications operators;

c) provides safeguards for authentication;

d) assesses the cost and resource implications to both the authorisation and postal or telecommunications operator.

**Corporate Governance Group**

5.5. The Corporate Governance Group will consider internal reports on the use of RIPA on a quarterly basis to ensure that the Council is using its powers consistently with this policy and that the policy remains fit for purpose. However, they will not be involved in making decisions on specific authorisations.

**Councillors**

5.6. Officers will consult councillors during the annual review of this policy. The Leader will receive a copy of the quarterly report to Corporate Governance Group.

5.7. **Authorising Officers**

The Authorising Officers must keep the relevant lead councillor informed of operations they are authorising. However, they must only provide an anonymised summary. Responsibilities during the authorisation process are set out in detail in 8.3.

## 6. COMPLAINTS

6.1. Complaints regarding Covert Surveillance must be directed to the SRO.

6.2. In order to maintain separation of duties, the officer who authorised the Covert Surveillance activity subject to a complaint must not carry out the investigation into the complaint.

6.3. The SRO may review the conduct of particular operations at any time.

# PART 2

## 7. SUMMARY OF THE AUTHORISATION PROCEDURE

7.1. The following is an overview. A more detailed description, together with an explanation of specific terms, is contained in the detailed procedures that follow.

| | |
|---|---|
| i. | Investigating officers must obtain a unique reference number from the RIPA Coordinating Officer for any planned, covert operation for which they intend to apply for authorisation. |
| ii | **Directed surveillance and sources**<br><br>Wherever possible, investigating officers must submit applications for authority to a designated Authorising Officer (see Part 3, Appendix A).<br>An up-to-date list of Authorising Officers and further advice can be obtained from the Information Rights Officer (IRO) or Data Protection Officer (DPO).<br><br>Where a likely consequence of surveillance is the acquisition of Confidential Material, the investigating officer must, always seek authority from the Managing Director or, in his or her absence, the Acting Managing Director.<br><br>Applications for the renewals and cancellations of surveillance must be authorised by the same authorising officer where this is possible.<br><br>**Communications Data**<br>Investigating officers must pass applications for communications data to the IRO or the Investigations Manager, who will administer the application and liaise with the Authorising Officer.<br><br>In all cases, the current forms provided by the Home Office must always be used. |
| iii | Authorising Officers (*not the investigating officer*) must document, on the authorisation form, their consideration of the proportionality and necessity of each exercise. |
| iv | Once authorised, the Authorising Officer will ensure that the administration at the Magistrates Court is contacted to arrange a hearing for judicial approval (the current *Application for judicial approval* form, as published by the Home Office, must be used for this purpose. |
| v | Investigating Officers must keep appropriate records of their investigation in line with established retention periods. They must forward a copy of all authorisations (including judicial approval form), reviews, renewals and cancellation forms, duly authorised (or where relevant, rejected), to the RIPA Coordinating Officer for inclusion in the central record as soon as possible. Forms will remain on the central record for three years from date of cancellation. |
| vi | The RIPA Coordinating Officer must provide a quarterly report to the Corporate Governance Group summarising authorisations to date and highlighting any areas of concern. The Leader of the Council will also receive a copy of this report. |

## 8. AUTHORISATION OF SURVEILLANCE

### 8.1. Activity requiring authorisation

8.1.1. Authorisation is required for the following activities (Please see the definitions in Appendix B):

- directed surveillance,
- use of sources ('covert human intelligence sources') and
- the acquisition or disclosure of communications data

8.1.2. Officers undertaking investigations on behalf of the Council must seek authorisation in writing for any of the above activities. The authorisations must be set out on the latest forms as published by the Home Office. The forms should not be adapted or modified unless authorised by the SRO.

### 8.2. Unique Reference Numbers (URNs)

8.2.1. Each application for authorisation must have a Unique Reference Number (URN). The officer applying for authorisation must first obtain the next available URN from the RIPA Coordinating Officer. Rejected forms will therefore also have URNs.

### 8.3. Authorising Officers – roles and responsibilities

8.3.1. Only specified senior managers may authorise covert surveillance (see Part 3, Appendix A). The Managing Director will inform those that may do so in writing. The Managing Director must approve all proposed changes to the delegation arrangements as far as they relate to any activities covered by this policy and procedure document. The Council's Authorising Officers are identified on the Intranet together with this policy and in the Council's Constitution.

8.3.2. Authorising Officers are responsible for overseeing each investigation and ensuring investigating officers follow the procedures set out in this document.

8.3.3. Authorising Officers cannot further sub delegate their powers to authorise covert surveillance.

8.3.4. Authorising Officers must not grant authorisation unless they believe it is necessary and proportionate *for the purpose of preventing or detecting crime or preventing disorder.* The Council may not use directed surveillance powers under RIPA except in relation to offences attracting a maximum sentence of at least six months' imprisonment or are related to the underage sale of alcohol or tobacco. See section 9 for guidance on the necessity and proportionality test.

### 8.4. Authorising the acquisition of Confidential Material *(see Appendix B for definition)*

8.4.1. The investigating officer must seek authority from the Managing Director, or, in his or her absence, the Acting Managing Director. The fullest consideration must be given to any cases where the subject of the surveillance might reasonably expect a high degree of privacy.

8.4.2. Applications in which the surveillance is likely to result in the acquisition of confidential material will be considered only in exceptional and compelling circumstances. The investigating officer must have full regard to the proportionality issues this raises.

**8.5. Authorisation for the use of sources**

8.5.1. A source may include those referred to as agents, informants and officers working undercover. Appendix C contains advice on how to identify whether your investigation includes the use of a source.

8.5.2. An Authorising Officer must not grant an authorisation for the use or conduct of a source unless there is a person with the responsibility for maintaining a record of the use made of the source at all times.

8.5.3. The Authorising Officer shall ensure that arrangements are in place for the proper oversight and management of sources, including appointing individual officers for each source. The Authorising Officer shall carry out a risk assessment before authorising the source. The risk assessment should include provisions for the safety and welfare of the source, and as such should be updated throughout the duration of the authorisation.

8.5.4. The person responsible for the day-to-day contact between the public authority and the source will usually be of a rank or position below that of the Authorising Officer.

8.5.5. Officers using a source shall consider the safety and welfare of that source (even after cancellation of the authorisation), and the foreseeable consequences to others of the tasks they are asked to carry out.

8.5.6. The Authorising Officer shall have regard to the special safeguards and provisions that apply to vulnerable individuals and juvenile sources, set out in more detail in the Covert Human Intelligence Source Code of Practice published by the Home Office at http://www.security.homeoffice.gov.uk.

8.5.7. Only the Managing Director or, in his or her absence, the Acting Managing Director is able to authorise the use of vulnerable individuals and juvenile sources (see Appendix E for special requirements for juveniles).

**8.6. Authorising acquisition of communications data**

8.6.1. Applications to obtain communications data will be submitted on the current Home Office forms to the National Anti-Fraud Network (NAFN) service. Investigating officers should contact the RIPA Coordinating Officer or, in the case of Benefit Fraud investigations, the Investigations Manager in the first instance for advice on the current procedure.

8.6.2. Once the authorisation has judicial approval, it will last for one month.

8.6.3. Communications data, and all copies, extracts and summaries of it must be handled and stored securely.

8.6.4. Officers must observe the requirements of the Data Protection Act 1998 and the principles of the Criminal Procedure and Investigations Act 1996. Officers must seek advice when they have questions about information security and integrity.

## 8.7. Communications Data – Special Procedure

8.7.1. There are two ways of authorising access to communications data;

- Through a Section 22(3) authorisation: An authorisation would allow the Council to collect or retrieve the data itself, or

- By a Section 22(4) notice: This is given to a postal or telecommunications operator and requires that operator to collect or retrieve the data and provide it to the council.

8.7.2. An Authorising Officer decides whether or not an authorisation should be granted or a notice given.

8.7.3. In order to illustrate, a Section 22(3) authorisation may be appropriate where:

- the postal or telecommunications operator is not capable of collecting or retrieving the communications data;
- it is believed the investigation may be prejudiced if the postal or telecommunications operator is asked to collect the data itself;
- there is a prior agreement in place between the authority and the postal or telecommunications operator as to the appropriate mechanisms for the disclosure of data.

8.7.4. Only Council officers may make applications for the obtaining and disclosure of communications data.

8.7.5. Notices and authorisations for communications data must be submitted through the NAFN – please contact the IRO or the Investigations Manager for more information.

## 8.8. Social Media

In some investigations, social media sites can form a useful source of intelligence. Usually a review of open source sites will not need authorisation. However, if reviews are carried out on the same individual with some regularity, this may amount to directed surveillance and authorisation should be obtained.

In cases where authorisation is not required, a Privacy Impact Assessment must be carried out beforehand to ensure that any accessing of data must be necessary and proportionate. If the surveillance relates to an employee, then reference should be made to the **ICO Employment Practices Code**.

If it is necessary and proportionate for the Council to covertly breach privacy controls (e.g. by becoming an account holder's "friend" using a false identity) to conduct an investigation, then a directed surveillance authorisation will be required. A register detailing identities used and by whom should then be created. The Authorising Officer should be kept informed about the progress of all such operations.

If the surveillance involves more than merely reading the sites contents, then an authorisation for the use and conduct of a CHIS will be required (see section 12.3).

**8.10. Applying for judicial approval**

8.10.1. This is obtained as soon as possible after authorisation by one of the Council's designated officers as described above and is required for authorisation applications and renewals (not internal reviews or cancellations)

8.10.2. The authorising officer should take steps to contact Her Majesty's Courts and Tribunals Service (HMCT) administration at the magistrates' court to arrange a hearing. The authorising officer may delegate this to the investigating officer.

8.10.3. The hearing is a legal proceeding and so officers must be formally designated to attend, be sworn in and present evidence or information as required. It is envisaged the investigating officer will usually attend as they will have the detailed knowledge required to answer the questions that might be raised. However, it is important to note that the forms and supporting papers must, by themselves, make the case for authorisation.

8.10.4. The magistrate should have sight of the authorisation form and the supporting documents setting out the case – that is, all information the authorisation relied on. However, the Council must retain the original documentation.

8.10.5. The magistrate must be provided with a partially completed judicial application form and they will complete the order section of the form and this will be the official record of the magistrate's decision.

8.10.6. Where renewals are timetabled to fall outside of court hours, it is the Council's responsibility to ensure the renewal is completed ahead of the deadline.

**8.9. Training**

8.9.1. The SRO is responsible for ensuring relevant members of staff are suitably trained as Authorising Officers and 'applicants', so as to avoid common mistakes appearing on forms for RIPA authorisations.

8.9.2. Training will be given, or approved by the SRO, before Authorising Officers are certified to sign any RIPA forms. A certificate of training will be provided to the individual and a central register of all those individuals who have undergone training or a one-to-one meeting with the SRO on such matters, will be kept by the RIPA Coordinating Officer.

**8.10. Activities by other Authorities**

8.10.1. Care is needed to ensure that there is no conflict between the activities of this Council and other public authorities. The investigating officer should make enquiries of other public authorities (e.g. the police) to find out whether they are carrying out similar activities if he or she considers that there is such a possibility.

**8.11. Joint Investigations (collaborative working)**

8.11.1. When some other agency has been instructed on behalf of the Council to undertake any action under RIPA, this document and the forms in it must be used (as for the normal procedure) and the agency advised or kept informed of the various requirements. They must be made aware explicitly of what they are authorised to do.

8.11.2. When some other agency (e.g. police, Customs & Excise, Inland Revenue and so on) wishes to use:

(a) the Council's resources (e.g. CCTV surveillance systems), that agency must use its own RIPA procedures. Before any officer agrees to allow the Council's resources to be used for the other agency's purposes, he must obtain a copy of that agency's RIPA form for the record and/or relevant extracts which are sufficient for the purposes of protecting the Council and the use of its resources.

(b) the Council's premises for their own RIPA action, the officer should normally co-operate unless there are security, or other good operational or managerial, reasons as to why the Council's premises should not be used for the agency's activities. In such cases, the Council's own RIPA forms should not be used as the Council is only assisting and not being involved in the RIPA activity of the external agency.

8.11.3. In terms of (a), if the police or another agency wish to use the Council's resources for general surveillance (as opposed to specific covert investigations), they must provide a letter requesting the proposed use. This must include the remit, duration, details of who will be undertaking the general surveillance and the purpose of it before any Council resources are made available. A copy of this letter must be provided to the RIPA Coordinating Officer for the central record.

## 9. THE 'NECESSARY & PROPORTIONATE' TEST

### 9.1. Responsibility for the test

9.1.1. An Authorising Officer shall not grant an authorisation unless he believes:

a) that an authorisation is necessary and

b) the authorised investigation is proportionate

9.1.2. When deciding whether the surveillance is necessary and proportionate, the Authorising Officer must consider the following:

### 9.2. "Necessary"

9.2.1. The exercise is deemed "necessary" if it is for the purpose of preventing and detecting a serious crime. A serious crime would attract a maximum sentence of at least six months' imprisonment.

### 9.3. "Proportionate"

9.3.1. The exercise is not "proportionate" if it is excessive in the overall circumstances of the case. The Authorising Officer would therefore need to explain the specific circumstances of each investigation, including whether the scale of the operation, the methods used and the impact on privacy would be excessive in relation to the allegation.

9.3.2. The proposed exercise and the methods used in the operation must meet the objective in question and must not be arbitrary or unfair nor must the impact on any individuals or group be too severe.

9.3.3. The Authorising Officer must explain why the methods used are the least invasive required to achieve the aims of the investigation and what other methods had been considered and why they were not implemented.

9.3.4. The authorising Officer must assess the risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation (see Collateral Intrusion below).

9.3.5. The Authorising Officer must give careful consideration to all of these points. They must demonstrate this on the authorisation form in the relevant parts.

9.3.6. Authorising Officers must exercise their minds every time they are asked to sign a form. They must never sign or 'rubber stamp' the form without thinking about their personal and the Council's responsibilities.

9.3.7. If the Authorising Officer believes that any boxes on the form/s are not relevant in a particular case, these must be clearly marked as being 'not applicable' or a line put through them.

9.3.8. The Authorising Officer must take great care to ensure they use accurate information and record it in the correct boxes. They must record reasons for any refusal of an application on the form so that there is a clear audit trail.

9.3.9. Authorising Officers should not be responsible for authorising investigations or operations in which they are directly involved.

### 9.4. Collateral Intrusion

9.4.1. Before authorising investigative procedures, the Authorising Officer shall take into account the risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation (collateral intrusion).

9.4.2. The investigating officer shall take measures, wherever practicable, to avoid or minimise unnecessary intrusion into the lives of those not directly connected with the investigation or operation.

9.4.3. An application for an authorisation shall include a risk-assessment of any collateral intrusion. The Authorising Officer shall take this into account, when deciding whether the surveillance is proportionate.

9.4.4. Where an operation unexpectedly interferes with the privacy of individuals who were not the subject of surveillance or covered by the authorisation in some other way, the investigating officer should inform the Authorising Officer.

## 10. DURATION, REVIEWS, RENEWALS AND CANCELLATION OF AUTHORISATIONS

### 10.1. Duration

10.1.1. Authorisations last for:

a) three months from date of grant or latest renewal for directed surveillance
b) 12 months from date of written grant for the conduct or use of a source
c) one month from date of written notice or authorisation for communications data, or earlier if cancelled under Section 23(8) of the Act.

10.1.2. Officers should note that the authorised period starts from the date authorisation is granted – not from the date the surveillance begins.

10.1.3. Authorisations must not expire. They must be kept under review, and then renewed or cancelled if no longer required.

### 10.2. Reviews

10.2.1. The Authorising Officer must review the operation by the date he or she has entered on the authorisation form (or latest renewal, if applicable). The purpose of the review is to assess the need for the surveillance to continue, taking into account the specific circumstances and sensitivities of the investigation. They must cancel the authorisation if it is no longer needed.

10.2.2. The Authorising Officer should record the results of the review on the standard review form and ensure they add a copy to the central record of authorisations held by the RIPA Coordinating Officer.

10.2.3. Where the surveillance provides access to confidential or sensitive information or involves collateral intrusion the officer should conduct reviews more frequently.

### 10.3. Renewals

10.3.1. Authorisations may be renewed more than once, if necessary, and the renewal should be kept and recorded as part of the central record of authorisations.

10.3.2. Authorisations can be renewed in writing shortly before the maximum period has expired. The renewal will begin on the day when the authorisation would have expired.

10.3.3. An authorisation cannot be renewed after the authorised period has expired. In this case, the Authorising Officer must cancel the authorisation and consider the matter afresh, taking into account the benefits of the surveillance to date and any collateral intrusion that has occurred.

10.3.4. The Authorising Officer who granted or last renewed the authorisation must cancel it if he or she is satisfied that the investigative procedure no longer meets the criteria upon which it was authorised.

10.3.5. Standard renewal forms for the authorisation of directed surveillance and CHIS are available on the Intranet and from the Home Office website.

### 10.4. Cancellations

10.4.1. An Authorising Officer must cancel an authorisation as soon as it is no longer necessary, or the conduct is no longer proportionate to what is sought to be achieved. The duty to cancel a notice falls on the Authorising Officer who issued it.

10.4.2. In the case of a notice issued in respect of communications data, the relevant postal or telecommunications operator must be informed of the cancellation.

10.4.3. The standard Home Office cancellation forms should be used

## 10.5. THE CENTRAL RECORD

10.6. The RIPA Coordinating Officer will maintain a central register of covert surveillance and use of sources in order to comply with legal requirements and for quality assurance purposes.

10.7. Authorising Officers must ensure copies of the following documents are included in the Council's central record:

1. Authorisation Forms (whether or not the authorisation is granted or refused)
2. Review forms
3. Renewal forms
4. Cancellation forms

10.8. The central record shall contain the following information for each case:

a) the type of authorisation or notice
b) the date the authorisation or notice was given;
c) name and rank/grade of the Authorising Officer;
d) the unique reference number (URN) of the investigation or operation;
e) the title of the investigation or operation, including a brief description and names of subjects, if known;
f) if the authorisation or notice is renewed, when it was renewed and who authorised the renewal, including the name and rank/grade of the Authorising Officer;
g) whether the investigation or operation is likely to result in obtaining confidential information;
h) the date the authorisation or notice was cancelled.
i) where and when a Justice of the Peace or Magistrate has granted authorisation

10.9. These records will be retained for a period of at least three years from the ending of the cancellation. A record will be kept of the dates on which the authorisation notice is started and cancelled.

10.10. Authorising Officers must provide the relevant forms to the RIPA Coordinating Officer within 1 week of the authorisation, review, renewal, cancellation or rejection.

10.11. Authorising Officers must ensure that copies of any forms, sent through the internal postal system, are in sealed envelopes using the security measures required for documents classified as Official-Sensitive.

10.12. This record will be monitored and appropriate advice given from time to time. The record will also be made available to the relevant Commissioner or an Inspector from the Investigatory Powers Commissioner's Office.

10.13. Each Investigating Officer must retain the original form with the working file of the investigation.

## 11. RECORDS RETENTION AND DESTRUCTION

### 11.1. Retention of material obtained through surveillance

11.1.1. Arrangements must be in place for the handling, storage and destruction of material obtained using covert surveillance, a source or the obtaining or disclosure of communications data. The Authorising Officer must make the following arrangements to protect the material:

- A named officer responsible for retaining the information and disposing of the information in a secure manner.
- Physical, technical and organisational measures must have been put in place to prevent unauthorised access to and use of the information obtained by the surveillance exercise.
- Physical, technical and organisational measures must have been put in place to prevent accidental or unauthorised loss of the information obtained by the surveillance exercise.

11.1.2. Authorising Officers must ensure compliance with data protection and local documented working procedures relating to the handling and storage of material.

11.1.3. Material obtained from properly authorised surveillance or a source may be used in other investigations. Where the product of surveillance could be relevant to pending or future proceedings, it should be retained in accordance with established disclosure requirements for a suitable period and subject to review.

### 11.2. Records maintained by the Investigating Officer

11.2.1. RIPA forms and any information collected by means of covert surveillance should be retained securely for **six years** after which the Authorising Officer must review whether the information should be disposed of or kept for a further length of time.

11.2.2. The Authorising Officer should take into consideration the status of any legal proceedings connected to the operation and the likelihood of any future legal action (including action taken by the subject(s) of the surveillance).

11.2.3. The justification for any decision to keep the information for longer than six years must be documented and kept with the file.

11.2.4. The following documentation must be kept but need not form part of the central record:

a) Supplementary documentation and notification of the approval given by the Authorising Officer;

b) Supporting documentation submitted when a renewal is requested;

c) the date and time when any instruction is given by the Authorising Officer.

### 11.3. Covert Human Intelligence Source Records (CHIS)

11.3.1. Investigating Officers must keep proper records of the authorisation and use of a source. The records shall contain the following information:

(a) the identity of the source;

(b) the identity, where known, used by the source;

(c) any relevant investigating authority other than the Council;

(d) the means by which the source is referred to within each relevant investigating authority;

(e) any other significant information connected with the security and welfare of the source;

(f) any confirmation made by a person granting or renewing an authorisation for the conduct or use of a source that the information in paragraph (d) has been considered and that any identified risks to the security and welfare of the source have where appropriate been properly explained to and understood by the source;

(g) the date when, and the circumstances in which, the source was recruited;

(h) the identities of the persons who, in relation to the source;

i. hold day-to-day responsibility for dealing with the source and for the source's security and welfare

ii. have a general oversight of the use made of the source (not to be the person identified in (h)(i))

iii. have responsibility for maintaining a record of the use made of the source

(i) the periods during which those persons have discharged those responsibilities;

(j) the tasks given to the source and the demands made of him in relation to his activities as a source;

(k) all contacts or communications between the source and a person acting on behalf of any relevant investigating authority;

(l) the information obtained by the conduct or use of the source;

(m) any dissemination of information obtained in that way; and

(n) in the case of a source who is not an undercover operative, every payment, benefit or reward and every offer of a payment, benefit or reward that is made or provided by or on behalf of any relevant investigating authority in respect of the source's activities for the benefit of that or any other relevant investigating authority.

(o) persons fulfilling the role of Handler and Controller with day-to-day responsibility for dealing with the source on behalf of the authority, and for the source's security and welfare must be identified and recorded as per section 29(5)(a) and (b) of the Regulation of Investigatory Powers Act.

# PART 3

**APPENDIX A**

**AUTHORISING OFFICERS**
Please check the Intranet for the most up to date list of Authorising Officers.

**Authorisations involving the acquisition of confidential material or the use of minors as sources:**
Authorising Officer 1 (TBC)
Authorising Officer 2 (TBC)

| **Designation** | **Name** |
|---|---|
| SRO | Steve White (until 12/02/18) |
| Authorising Officer 1 | Steve White (until 12/02/18) |
| Authorising Officer 2 | TBC |
| Managing Director | James Whiteman |
| | |

**APPENDIX B**

**DEFINITIONS**

**Communications Data**
This covers the obtaining of communications data and the disclosure to any person of such data. Communications data relates to a postal service or telecommunications system. For these purposes, communications data includes information relating to the use of a postal service or telecommunications system but does not include the contents of the communication itself, content of emails or interaction with websites.

Communications data includes subscribers' details, names, addresses, and telephone numbers of those contacted, billing addresses, account information, web addresses visited etc.

Two types of data (Customer Data or Service Data) are available to local authorities and, when making an application for obtaining or disclosing such data, the applicant must specify exactly which type of information is required from within each of the subscriber data and service use data.

a) Customer data – (Subscriber data, RIPA s21(4))

Customer data is the most basic. It is data about users of communication services.

This data includes:

- Name of subscriber
- Addresses for billing, delivery, installation
- Contact telephone number(s)
- Abstract personal records provided by the subscriber (e.g. demographic information)
- Subscribers' account information – bill payment arrangements, including bank, credit/debit card details
- Other services the customer subscribes to.

b) Service data – (Service Use data, RIPA s21(4)(b))

This relates to the use of the service provider's services by the customer, and includes:

- The periods during which the customer used the service(s)
- Information about the provision and use of forwarding and re-direction services by postal and telecommunications service providers
- 'Activity', including itemised records of telephone calls (numbers called), internet connections, dates and times/duration of calls, text messages sent
- Information about the connection, disconnection and reconnection of services

- Information about the provision of conference calling, call messaging, call waiting and call barring telecommunications services
- Records of postal items, such as records of registered, recorded or special delivery postal items, records of parcel consignment, delivery and collection
- 'Top-up' details for prepay mobile phones – credit/debit card, voucher/e-top up details

*A third type of data (traffic data) is not accessible to local authorities.*

**Confidential Journalistic Material**
This relates to material acquired or created for the purposes of journalism and subject to an undertaking to hold it in confidence, as well as communications resulting in information being acquired for the purposes of journalism and held subject to such an undertaking.

**Confidential Material**
This is information relating to an area where the subject of the investigation or operation might reasonably expect a high degree of privacy, or where confidential information is involved. Confidential information consists of matters subject to legal privilege, confidential personal information or confidential journalistic material.

**Confidential Personal Information**
This is information held in confidence relating to the physical or mental health or spiritual counselling concerning any identifiable individual (living or dead). This may include oral and written communications subject to an express or implied undertaking to hold the information in confidence.

Please note that the definition above applies only in the context of covert surveillance and differs from the definitions of sensitive personal information used in guidance on data protection matters.

**Covert**
In general, this is something carried out in a manner calculated to ensure that the subject of the surveillance is unaware of it.

**Covert Human Intelligence Source:** Key Features:
- Aims to establish a relationship (personal or otherwise) with another person for the covert purpose of obtaining information and/or disclosing it covertly.

**Directed Surveillance**:

Directed surveillance is surveillance which is covert (in other words, carried out in such a way that the subject would not know they are under surveillance), but not intrusive, and is undertaken:

a) for the purposes of a specific investigation or operation;
b) in such a manner as is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation); and
c) not as an immediate response to events or circumstances of such a nature that it would be unreasonable and impracticable for an authorisation under RIPA to be sought for the surveillance.

**Intrusive Surveillance**:
Directed surveillance turns into intrusive surveillance if carried out involving anything that occurs on residential premises or any private vehicle and involves the presence of someone on the premises or in the vehicle or is carried out by means of a surveillance device.

If the device is not on the premises or in the vehicle, it is only intrusive surveillance if it consistently produces information of the same quality as if it were.

Where surveillance is carried out by a device designed or adapted principally for the purpose of providing information about the location of a vehicle, the activity is directed surveillance.

Surveillance involving commercial premises and commercial vehicles does not fall within the definition of intrusive surveillance.

*Local authorities are **not** allowed to carry out intrusive surveillance.*

**Surveillance** includes:

a) monitoring, observing or listening to persons, their movements, their conversations or their other activities or communication;
b) recording anything monitored, observed or listened to in the course of surveillance; and
c) surveillance by or with the assistance of a surveillance device.

Surveillance includes the interception of postal and telephone communications where the sender or recipient consents to the reading of or listening to or recording of the communication. This is a form of directed surveillance.

**APPENDIX C**

**FURTHER GUIDANCE**

## Q.1. IS MY OPERATION 'DIRECTED SURVEILLANCE'?

Ask yourself the following questions:

### 1. Is the surveillance *covert*?

1.1. Covert surveillance is any surveillance carried out in a way calculated to ensure that the persons under surveillance are unaware it is taking place.

1.2. If your activities are not hidden from the subjects of your investigation, you are not within the RIPA framework at all. In many cases, Officers will be behaving in the same way as a normal member of the public (e.g. in the case of most test purchases), and/or will be going about Council business openly (e.g. a market inspector walking through markets).

1.3. Similarly, surveillance is overt if the subject has been told it will happen - e.g. where a noisemaker is warned (preferably in writing) that noise will be recorded if it continues, or where an entertainment licence is issued subject to conditions, and the licensee is told that officers may visit without notice or identify themselves to the owner to check that conditions are being met.

1.4. It should be noted that if the same outcome can be achieved by overt means then those means need to be fully explored in the first instance. Covert surveillance must only be undertaken when there is no less invasive way of achieving the outcome.

### 2. Is the surveillance for the purposes of a specific investigation or a specific operation?

2.1. The provisions of the Act do not normally cover the use of overt CCTV surveillance systems (such as those operated by Car Parks or the Safer Guildford Partnership), since members of the public are aware that such systems are in use. However, there may be occasions when the council wishes to use overt CCTV systems for the purposes of a specific operation – eg if the cameras are targeting a particular known offender. In such cases, authorisation for directed surveillance may be necessary. The procedure for the use of overt CCTV for a covert operation is covered in a separate protocol document.

### 3. Is the surveillance to be carried out in such a manner that it is likely to result in the obtaining of private information about a person?

3.1. Private information includes any information relating to a person's private or family life. Private information should be broadly interpreted to include an individual's private or personal relationship with others. It includes an individual's business and family relationships. Family life should be treated as extending beyond the formal relationships created by marriage.

### 4. Is the surveillance otherwise than by way of an immediate response to events or circumstances where it is not reasonably practicable to get authorisation?

4.1. *Directed surveillance* does not include covert surveillance carried out by way of an immediate response to events or circumstances which, by their very nature, could not have been foreseen. For example, a police officer would not require an authorisation to conceal himself and observe a suspicious person that he came across in the course of a patrol.

4.2. However, if as a result of that immediate response, you decide to undertake a specific investigation you will then need authorisation.

**Q.2. AM I USING A COVERT HUMAN INTELLIGENCE SOURCE?**

1. A person is a source if:

   a) He establishes or maintains a personal or other relationship with a person for the covert purpose of assisting anything falling within paragraph (b) or (c);
   b) He is covertly using such a relationship to obtain information or to provide access to any information to another person; or
   c) He is covertly disclosing information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

2. A source may include those referred to as agents, informants and officers working undercover.

3. Such a purpose is 'covert', if and only if, the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose.

4. A relationship is used covertly, and information obtained is disclosed covertly, if and only if it is used or disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question.

5. The use of a source involves inducing, asking or assisting a person to behave as a source, or to obtain information by means of the behaviour of such a source.

6. This covers the use of professional witnesses to obtain information and evidence. For example, it will include professional witnesses engaged by Housing to pose as tenants to obtain information and evidence against alleged nuisance perpetrators.

7. Carrying out test purchases will not require the purchaser to establish a relationship with the supplier with the covert purpose of obtaining information and, therefore, the purchaser will not normally be a CHIS. For example, authorisation would not normally be required for test purchases carried out in the ordinary course of business (eg walking into a shop and buying a product over the counter). By contrast, developing a relationship with a person in the shop, to obtain information about the seller's suppliers of an illegal product will require authorisation as a CHIS. Similarly, using mobile hidden recording devices or CCTV cameras to record what is going on in the shop will require authorisation as directed surveillance.

8. The Code of Practice states that the provisions of RIPA are not intended to apply in circumstances where members of the public volunteer information to the police or other authorities, as part of their normal civic duties, or to contact numbers set up to receive information (such as Crimestoppers, Customs Confidential, the Anti-

Terrorist Hotline, or the Security Service Public Telephone Number). Members of the public acting in this way would not generally be regarded as sources.

9. An authorisation under RIPA will provide lawful authority for the use of a source.

**APPENDIX D**

**FURTHER EXAMPLES TO HELP YOU DECIDE WHETHER YOUR ACTIVITIES ARE COVERED BY THIS POLICY**

Firstly, consider:

- Is it necessary for the operation to be covert? Could you obtain the evidence you require without resorting to Covert Surveillance? Authorising Officers should consider this very seriously because, if it is found that there was no need to carry out the surveillance covertly, the invasion of privacy may be deemed disproportionate to the investigation in question.

- *Overt* investigations (that is, not carried out in a manner calculated to ensure that the subject is unaware of the operation) is not subject to the authorisation procedures set out in this policy. Overt activity includes (but is not limited to) routine patrols, observation at trouble spots, immediate response to events and overt use of CCTV.

**Examples:**

**Does the investigation involve the collection of private information?**

1. Two people holding a conversation on the street or in a bus may have a reasonable expectation of privacy over the contents of that conversation even though they are associating in public. The contents of the conversation should be considered as private information.

   The offence under investigation would need to meet the minimum penalty criteria and a directed surveillance authorisation would be necessary to listen in to or record the conversation as part of a specific investigation or authorisation. (Source: Covert Surveillance and Property Interference Revised Code of Practice 2010)

2. A surveillance officer intends to record a specific person providing their name and telephone number to a shop assistant, in order to confirm their identity, as part of a criminal investigation.

   Although the person has disclosed these details in a public place, there is a reasonable expectation that the details are not being recorded separately for another purpose. Before proceeding, the investigating officer should make sure the alleged offence meets the minimum penalty criteria and seek a directed surveillance authorisation. (Source: *Covert Surveillance and Property Interference Revised Code of Practice 2010*).

**Planning Enforcement**

1. Routine activities such as Enforcement Officers looking at new building work, which has not been granted planning permission.

   This is not directed surveillance, but falls under normal enforcement duties. Section 80 of the Regulation of Investigatory Powers Act 2000 provides a general saving for collecting information by lawful means such as this. However, such routine activities should not develop into directed surveillance.

2. Officers wish to drive past a café to obtain a photograph of the exterior.

Reconnaissance of this nature is unlikely to require a directed surveillance authorisation. However, if the exercise was to establish a pattern of occupancy of the premises by someone, the accumulation of the information is likely to result in private information. In the latter case, a directed surveillance authorisation would be required and the offence would need to meet the minimum penalty requirements. (Source: *Covert Surveillance and Property Interference Revised Code of Practice 2010*).

3. You are conducting a site visit in response to a report made by a member of the public who suspects a change of use of land, which is likely to involve criminal activity. The circumstances suggest that you will need to monitor the site in a covert manner and you are likely to obtain private information about the owner and/or collateral information about other users of the site such as workers.

   This activity appears to fall within the definition of Directed Surveillance. However, it is not legal to use covert surveillance to investigate crimes that would attract a custodial sentence with a minimum term of less than six months. You must therefore find some overt method of dealing with the offence.

4. You are unable to gather conclusive evidence that illegal activity is taking place on site but you still suspect that it is. Therefore, you decide to observe the site by driving past it periodically over the next fortnight. If you see unauthorised work taking place you will take a photo – but not covertly.

   This does not appear to fall within the definition of either Directed Surveillance or Covert Human Intelligence Sources. This low-level activity is <u>not</u> subject to the authorisation procedures set out in this policy.

**Benefit Fraud**

5. You are required to investigate an allegation that Mr X is claiming housing and council tax benefit even though he has been working full time for a number of years. Mr X did not declare on his benefit application that he had been working. You therefore intend to covertly observe his activities at his alleged employer's address in order to establish if he is working there. The observation will be from a vehicle and will cover a number of days.

   This appears to involve the systematic surveillance of an individual and falls within the definition of Directed Surveillance, as set out in Appendix B, for the following reasons:

   - The surveillance is being carried out for the purposes of a specific investigation into Mr X's alleged benefit fraud.
   - The surveillance is of Mr X's personal activities and is therefore likely to produce private information about him.
   - The exercise is not an immediate response to events or circumstances but has been planned in respect of timing and the manner in which the surveillance is to be carried out.
   - It is likely that collateral material will be gathered

**Employer Responsibilities**

6. Recurrent thefts from staff are taking place and after considering all of the options, it has been suggested that the only recourse is to set up a secret CCTV camera covering the work area to catch the culprit "in the act".

Normal business practice (in other words the kinds of responsibilities that all employers would have in relation to staff) are outside of the RIPA controls. Therefore, the operation would need to be conducted in accordance with the Data Protection Act 1998 and the Privacy Impact Assessment (PIA) provisions within that legislation. Use the PIA template available on the Intranet.

You would need to consider all of the circumstances of the case. But where the aim is to stop the offending behaviour, overt measures (such as overt CCTV) may be more proportionate.

**Note:** If a crime on Council premises were being investigated by the police and they are conducting the surveillance, they would be required to authorise the surveillance, not the Council.

7. A manager has received a report from employee A that employee B is spending hours surfing the internet. The manager wishes to obtain a print out of employee B's websites visited and times spent on the internet to check whether the allegations are true.

   As with the scenario above, this investigation would fall outside of the RIPA provisions. The Council has arrangements to ensure any staff investigations involving ICT equipment are necessary and proportionate. Please use the Privacy Impact Assessment form available as part of the Acceptable Use Policy and available on the Data Protection and Information Security intranet page

   **Note:** Automatic and untargeted central monitoring of internet and email use carried out by ICT software, which would highlight obvious infringements of the Council's Acceptable Use Policy is allowed under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

**Housing Management**

8. A member of the public reports that their neighbour's garden is a health hazard. You visit the site, which contains excessive rubbish and materials that are clearly likely to be an environmental hazard to the local community. As the tenant is not at home, you take a photograph of the view of the garden from the road. You have not deliberately planned that the photograph should be taken without the knowledge of the tenant concerned and any future surveillance of the site will not be carried out in a manner calculated to ensure that the tenant is unaware of it.

   This does not appear to fall within the definition of either Directed Surveillance or Covert Human Intelligence Sources as set out in Appendix A and is therefore <u>not</u> subject to the authorisation procedures set out in this policy. However, care will be required if photos are taken whilst on the premises as this may in some circumstances become "Intrusive Surveillance", which the Council does not have the authority to carry out.

   If you gather personal data (information that can be used to identify someone), this will be subject to the Data Protection Act and the activity would be subject to a Privacy Impact Assessment.

9. You have received an application for housing by someone claiming to be homeless. However, you have grounds to believe that the claim is fraudulent, so you wish to carry out surveillance of the claimant's suspected residence to establish the integrity of their application.

This appears to fall within the definition of Directed Surveillance, as set out in Appendix B, for the following reasons:

- The surveillance is being carried out for the purposes of a specific investigation into a fraudulent application.
- The surveillance is likely to produce private information about him as well as collateral information about third parties.
- The exercise is not an immediate response to events or circumstances but has been planned in respect of timing and the manner in which the surveillance is to be carried out.
- However, you would need to consider whether the offence is listed on the statute book as attracting a minimum custodial sentence of six months or more before proceeding with the covert elements of the investigation and applying for authorisation.

**Use of CCTV**
An officer receives information that an individual suspected of Benefit Fraud will be going to their workplace, in the High Street and within an area monitored by CCTV. The officer wishes to use the CCTV system to obtain evidence that the suspect is working.

This is targeted use of the town centre's overt CCTV system, to conduct surveillance against that individual without his being aware that there is a specific interest in him. The investigating officer would need to apply for an authorisation for directed surveillance.

If you are investigating a serious criminal matter and you are unsure if your surveillance activity falls under RIPA, you should apply for authorisation in order to avoid any claim that Guildford Borough Council has infringed anyone's Human Rights, which could disqualify the evidence from being permitted in court.

**APPENDIX E**

**COVERT HUMAN INTELLIGENCE SOURCES – USING MINORS OR VULNERABLE PEOPLE**

The Regulation of Investigatory Powers (Juveniles) Order 2000 S.I. 2000/2793 states that:

- A Source under 16 years of age cannot be used to obtain information about his/her parent or anyone with parental responsibility.

- Where a source is under 16, someone must have responsibility for ensuring than an appropriate adult is present at meetings (i.e. parent, guardian, a person who has assumed responsibility for his/her welfare, anyone over 18 who is not employed by Guildford Borough Council).

- Where a source is under 18, no authorisation can be granted unless someone has carried out a risk assessment covering the likelihood of physical and psychological injury arising from the covert activities AND is satisfied the risks are justified AND have been properly explained AND understood by the source.

- Where the operation or investigation relates to a parent or guardian, the authoriser must be aware of that fact and give “particular consideration” to whether the authorisation is justified.

- Where the source is under 18, at the time of authorisation it can only last one month before being renewed.

- Authorisation for the use of a juvenile or vulnerable person CHIS must be authorised by the Managing Director or, in their absence, the Executive Head of Governance.

**APPENDIX F**

**FORMS**
**The latest versions of the forms listed below should be downloaded from the Home Office (https://www.gov.uk/government/collections/ripa-forms--2)**

Application for authorisation of directed surveillance
Review of directed surveillance
Renewal of directed surveillance
Cancellation of directed surveillance

Application for CHIS
Review of CHIS
Renewal of CHIS
Cancellation of CHIS

Application for communications data

Application for judicial approval