COVERT SURVEILLANCE AND ACCESS TO COMMUNICATIONS DATA POLICY AND GUIDANCE NOTES

Scope

This policy document explains how the Council's officers will comply with the Regulation of Investigatory Powers Act 2000 (RIPA) and the Investigatory Powers Act 2016 in relation to directed surveillance, use of covert human intelligence sources and the acquisition of communications data.

This policy is supplementary to the legislation, the statutory code of practice and the Home Office guidance to local authorities in England and Wales on the judicial approval process for RIPA and the crime threshold for directed surveillances.

RIPA Senior Responsible Officer: Chief Executive

RIPA Co-ordinating Officer: Gary Rowland (Senior Legal Adviser, Corporate Governance)

Revised: February 2024
Review date: February 2025

CONTENTS

POLICY STATEMENT

The Regulation of Investigatory Powers Act 2000 (RIPA) provides the legislative framework within which covert surveillance must be conducted whilst the Investigatory Powers Act 2016 provides the legislative framework within which access to communications data operations must be conducted. This ensures that investigatory powers are used with minimal interference with an individuals human rights. This Policy Statement is intended as a practical reference guide for Council Officers who may be involved in such operations.

This Policy is supplementary to the:

- Home Office guidance on the use of covert surveillance or covert human intelligent sources (CHIS) - https://www.gov.uk/government/publications/covert-surveillance-and-covert-human-intelligence-sources-codes-of-practice

- Regulation of Investigatory Powers Act (RIPA) 2000 - http://www.legislation.gov.uk/ukpga/2000/23/contents

- Investigatory Powers Act 2016 - https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted

The Council is committed to implementing the provisions of RIPA to ensure that any covert surveillance and/or access of communications data that is carried out during the course of investigations is undertaken properly and that the activity is necessary and proportionate to the alleged offence(s). Following the implementation of the Protection of Freedoms Act 2012 investigatory powers can only be used in relation to activities that would receive a minimum sentence of six months imprisonment or are in relation to the underage selling of alcohol or tobacco. If such action is contemplated initial consultation with the Council's Co-ordinating Officer should be undertaken at the earliest opportunity.

The Council seeks to ensure that this Policy Statement remains consistent with the Council's objectives.

This Policy ensures:

- that proper procedures are in place in order to carry out covert surveillance or to obtain communications data;
- that an individual's right to privacy is not breached without justification;
- that proper authorisation is obtained for covert surveillance or access to communications data;
- that proper procedures are followed; and
- that covert surveillance is considered as a last resort, having exhausted all other options.

1. BACKGROUND

Scope and Control

1.1 RIPA is the law which governs the use of a number of covert techniques for investigating crime and terrorism. Using covert techniques allows public authorities, which range from the police and security agencies to local authorities and organisations, such as the Office of Fair Trading, to investigate suspected offences without alerting an individual that they are part of that investigation.

1.2 Local authorities can use three techniques. They can obtain **Communications Data,** use **Directed Surveillance** and use **Covert Human Intelligence Sources (CHIS).**

1.3 RIPA requires that an authorisation is needed for the use of these investigatory techniques and that they can only be used where it is considered proportionate and necessary to what is sought to be achieved.

1.4 Local authorities can only use these investigatory techniques if they are necessary to prevent or detect crime or prevent disorder.

1.5 These guidance notes provide a summary of the main points from the Home Office Covert Surveillance Code of Practice that are relevant to Swale Borough Council. They apply to authorisations for covert surveillance and access to communications data made by the Council.

1.6 To improve awareness, this guidance also briefly refers to activities that the Council has determined **should not** be undertaken.

1.7 Before undertaking any covert surveillance, these guidance notes should be read and if it is considered proportionate and necessary, further advice should be sought from the RIPA Co-ordinating officer. Members of the public who enquire about covert surveillance procedures should be referred to the Home Office Covert Surveillance Code of Practice. Officers employed by the Council and who are involved in covert surveillance should be made aware of these guidance notes and of the Code of Practice.

1.8 The use of the RIPA by the Council will be overseen by the Senior Responsible Officer supported by the Co-ordinating Officer. These positions are currently held by:

- Senior Responsible Officer – Larissa Reed (Chief Executive)
- Co-ordinating Officer – Gary Rowland (Senior Legal Advisor)

Senior Responsible Officer

The Senior Responsible Officer will have overall responsibility for the integrity of the RIPA process within the Council. In addition they will:

1. be responsible for the Council's compliance with RIPA and its regulatory framework;
2. engage with the Commissioners and Inspectors when they conduct inspections;
3. oversee the implementation of any recommendations made by the Investigatory Powers Commissioner's Office (IPCO);
4. carry out periodic oversight of the authorisations; and

5. report annually to Members on the usage of RIPA within the Council.

Co-ordinating Officer

The Co-ordinating Officer will be responsible for overseeing the day to day RIPA process, in particular they will:

1. keep the Central Record and collate the documentation received;
2. exercise the day to day oversight over the RIPA process by ensuring the quality of the documents submitted;
3. to monitor the Council's use of its appointed S.P.O.C agent, the National Anti Fraud Network ('NAFN');
4. monitoring the timeliness of the officers in making returns, carrying out reviews and effecting renewals and cancellations;
5. keep a record of the RIPA training programme as part of the Central Record; and
6. raise general RIPA awareness within the Council whilst ensuring that detailed awareness and training is provided to applicants and Authorising Officers in accordance with the IPCO recommended timeframes.

NB: applicants and Authorising Officers are required to undertake regular training at least once in every three year period.

Definitions

1.9 **Covert surveillance** is any surveillance carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place.

1.10 General observation forms part of the duties of the Council's enforcement officers i.e. **overt surveillance**, and is not usually regulated by RIPA (for example observations during routine planning enforcement matters where the property owner has been 'put on notice' that inspections may be carried out). Such observation may involve the use of equipment to merely reinforce normal sensory perception, such as binoculars, or the use of cameras, where this does not involve systematic surveillance of an individual.

1.11 The use of noise monitoring equipment to measure noise audible in a complainant's premises does not amount to covert surveillance because the noise has been inflicted by the perpetrator who it is likely has forfeited any claim of privacy. The use will only become covert when sensitive equipment is used to discern speech or other noisy activity that is not discernible to the unaided ear.

1.12 Although the provisions of RIPA do not normally cover the use of overt CCTV surveillance systems, since members of the public are aware that such systems are in use, there may be occasions when the Council's overt CCTV system is used for the purpose of a specific investigation or operation. Such cases should be discussed with the Authorising Officer who will decide whether it is directed surveillance and whether authorisation is required.

1.13 The primary purpose of surveillance is to secure evidence to bring offenders before the courts. The proper authorisation of surveillance should ensure the admissibility of such evidence in criminal proceedings.

1.14 **Directed surveillance** is the type of covert surveillance that the Council's employees will be permitted to undertake on an exceptional basis and only within the Council's

responsibilities for the prevention and detection of crime, or for the prevention of disorder. Authorisation for directed surveillance **must** first be obtained.

1.15 Directed surveillance is defined as surveillance which is covert, but not intrusive, and undertaken:

a) for the purpose of the prevention or detection of crime or to prevent disorder;

b) for the purpose of a specific investigation or specific operation;

c) in a manner that is likely to result in the obtaining of **private information** about a person (whether or not specifically identified for the purpose of the investigation or operation). Private information is defined at paragraph 1.19 below; and

d) otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under Part II of the 2000 Act to be sought for the carrying out of the surveillance. For example, you may be in a Post Office obtaining information in relation to a particular customer when you observe a different person committing a benefit fraud. Officers acting in their line of duty are allowed to follow that person, if necessary, to establish their identification and any other information that may help with the subsequent investigation but you should not do so if you believe there is any possibility of a risk to your own safety.

1.16 A similar situation may occur whilst visiting an employer under section 110 powers, Social Security Administration Act 1992 (which requires separate authorisation). For example, if during a visit to an employer you recognise an individual benefit claimant, authorisation for watching the person working would not be required. This is because you have come across the information incidentally and in the course of your normal duties. However, if you visited an employer with the precise intention of observing an identified individual at work (whilst claiming benefit), written authorisation would be required before the visit.

1.17 Directed surveillance includes covert surveillance within office and business premises.

1.18 **Private information** includes:

a) any information relating to a person's private or family life, or

b) information relating to aspects of a person's professional and business life.

The concept of private information should be broadly interpreted to include an individual's private or personal relationship with others. Family life should be treated to extend beyond the formal relationships created by marriage.

1.19 **Intrusive surveillance** is defined as covert surveillance that:

a) is carried out in relation to anything taking place within any residential premises or any private vehicle; and

b) involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device or involves premises where legal consultations take place.

Under no circumstances should this type of surveillance be undertaken. An alternative means of obtaining the information should be sought.

1.20 **Interception of post, e-mail and recording of telephone conversations.** The interception of communications sent by post or by means of public telecommunications systems or private telecommunications systems attached to the public network are outside of the remit of Council officers.

1.21 **Covert Human Intelligence Source (CHIS)** is the term used for a person who is tasked by the Council to establish or maintain a relationship with a person for the purpose of covertly obtaining or disclosing information i.e. it is someone working "under cover" who has been asked to obtain information, to provide access to information or to otherwise act, incidentally for the benefit of the Council.

1.22 A relationship is established or maintained for a covert purpose if and only if it is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose.

1.23 A person is considered to be a CHIS if:

(a) they establish or maintain a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraphs (b) or (c) below;

(b) they covertly use such a relationship to obtain information or provide access to any information to another person; or

(c) they covertly disclose information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship.

1.24 **The Council has taken a policy decision that it will be the general practice not to undertake this type of surveillance activity**. An alternative means of obtaining the information should be followed. However, it is necessary that the Council be equipped to deal with CHIS should the situation arise.

1.25 If it is necessary to request an authorisation under CHIS, advice should first be sought from the RIPA Senior Responsible Officer.

1.26 As with directed surveillance the Council may only make an authorisation permitting the use of CHIS on the ground that it is necessary for the purpose of the prevention or detection of crime or the prevention of disorder.

1.27 It should be noted that where members of the public volunteer information to council officers, either as a complaint or as part of their civic duties i.e. use contact numbers set up for the reporting of suspected benefit fraud or for whistle-blowing etc. they would not generally be regarded as a CHIS. In addition, if someone is keeping a diary record of nuisance, this will not amount by itself to use of a CHIS. With the exception of a diary record of nuisance, a Council officer **must never** ask a member of the public to routinely record information relating to specified individuals on the Council's behalf.

1.28 In order for the Council to carry out surveillance using CHIS (should the need arise) it is necessary to have appropriately trained officers designated as Controllers and Handlers. These posts will carryout the following functions:

- Controller – will at all times have general oversight of the use made of the source.
- Handler – will have day to day responsibility for dealing with the source on behalf of the authority, and for the source's security and welfare.

In all cases the Controller will be the RIPA Senior Responsible Officer.

Handlers will include investigators and enforcement officers that have received the relevant CHIS training and have been authorised by the RIPA Senior Officer to undertake this role. A register of those authorised as handlers will be kept by the RIPA Co-ordingating Officer.

In addition to the above the RIPA Co-ordinating Officer will have responsibility for maintaing a record of the use made of the source.

1.29 **Accessing Communications Data**

Local Authorities can obtain communications data for investigating crime under the Investigatory Powers Act 2016. Communications data includes land line and mobile telephone subscriber and billing data for telephone, web and postal customers.

1.30 Communications data can be obtained where it is necessary and proportionate to do so. Applications are primarily used to identify or locate suspects. Examples include applications to ascertain subscriber identity and address details of illegal fly tipping suspects from mobile phone number evidence.

1.31 The Council has appointed NAFN to provide a RIPA Single Point of Contact (SPoC) service to obtain communications data. NAFN is authorised to carry out requests to telecommunications service providers for category B and C data (see 1.32) for criminal investigations. This includes subscriber and billing information on telephone, web and postal services.

1.32 It should be noted that in order for Local Authorities to seek authority to acquire category B data, it must meet the new serious crime threshold. A serious crime is one which carries a prison sentence for a minimum of 12 months and meets the definition set out in section 81(3)(b) of the Act, i.e. conduct that involves the use of violence, results in substantial financial gain or is conduct by a large number of persons in pursuit of a common purpose. Category C data can still be acquired for any crime where necessary and proportionate to do so.

Category Table

A Data – Not accessible to Local Authorities	B Data – Available if serious crime threshold met	C Data – Available
Cell site IEMI Incoming caller data	Itemised Billing Call Diversion Data Downloading Outgoing call data	Subscriber detail including: Name and Address Method of Payments Customer info.

NB: Local Authorities are not able to obtain Category A data.

Social Networking Sites

1.33 **Social Networking Sites (SNS)** which include but are not limited to Facebook, Instagram, Twitter and TikTok can provide information that will aid an investigation. When using these sites to carry out surveillance it is essential to know how they work and officers should not assume that one service provider works in the same way as another.

1.34 In all cases it would be unwise to assume that the content came from an open source or was publically available, even where security settings are low, as the author would have some reasonable expectation of privacy where access controls are applied.

1.35 When conducting any surveillance of social media sites use of an officers personal account is prohibited and advice should be sought from the Communciations Team with regards to setting up a Council account. It may pose a risk to an officers' personal safety when viewing social media profiles from a personal account, due to the potential for a 'digital footprint' to be left and therefore potentially identifying the officer to the account holder.

1.36 Where a site is being covertly accessed for monitoring purposes it may be necessary for an authorisation for directed surveillance to be obtained. As part of an investigation it is possible to take an initial look at an individuals social media activity, however, should there be a need to return to the site this may constitute surveillance. In such circumstances advice should be obtained from the RIPA Co-ordinating Officer before further surveillance is carried out.

1.37 When accessing an individuals' social media site, an officer of the Council must never establish or maintain a relationship with that individual without consulting with the SRO, as an authorisation for a CHIS may need to be obtained. See 1.23 above for full details of what constitutes a CHIS.

1.38 The Central Record will contain a register of any Council profiles utilised and a record of their use, where the Council decides to utilise Social Media for the purpose of investigation. The RIPA Co-ordinating officer must be involved prior to any social media being utilised for surveillance, to ensure appropriate records are being kept and stored.

1.39 A brief summary of the relevant legislation governing covert surveillance has been included at Appendix A.

2. GENERAL RULES ON AUTHORISATIONS

2.1 Where an authorisation or renewal is sought for the use of Directed Surveillance, acquisition of Communications Data or the use of CHIS it will be necessary to obtain Judicial Approval, i.e approval from the Magistrates Court. It will still be necessary to go through the internal authorisation stage, detailed below, prior to an application for Judicial Approval. The procedure for obtaining Judicial Approval is detailed at paragraphs 4.12 to 4.14 below.

NB: A flowchart produced by the Home Office showing the authorisation procedure is shown at Appendix B.

2.2 Directed Surveillance and CHIS

2.2.1 You must seek an authorisation where the surveillance is likely to interfere with a person's rights to privacy *(Article 8 of the European Convention on Human Rights)* by obtaining private information about that 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.

2.2.2 In the event that the Council is required to conduct joint directed surveillance working with another agency, the tasking agency should obtain the authorisation. For example, in the event that the police require covert surveillance by the Councils' CCTV system the police would normally seek the authorisation. A copy of the Authorisation, Renewal and Cancellation forms should be sought from the tasking agency to provide a record and justification for the Councils involvement. This should be presented to the RIPA Co-ordinating officer for recording.

2.3 Accessing Communications Data

2.3.1 Only authorised officers are able to use the NAFN Single Point of Contact service to access communications data. NAFN provides Council officers with access to a secure online system for processing RIPA telecommunications requests. Authorised applicants and designated persons can submit, approve and track applications through one central secure website. NAFN review all applications for legal compliance prior to approval from Swale's designated person. NAFN is subject to inspection by the officers of the Interception Commission to ensure compliance with RIPA.

2.4 RIPA Authorising Officers

The Authorising Officers for the Council are:

- Chief Executive / RIPA Senior Responsible Officer (SRO)
- Director of Regeneration / Deputy SRO
- Director of Resources
- Head of Environment and Leisure
- Head of Housing and Community Services

No person designated as an Authorising Officer may act as an Authorising Officer unless they have undertaken appropriate training.

In addition to the above the following officers will be responsible for the authorisation of NAFN RIPA telecommunications requests:

- Chief Executive / RIPA Senior Responsible Officer (SRO)

2.5 Necessity and Proportionality

2.5.1 Obtaining an authorisation for surveillance will only ensure that there is a justifiable interference with an individual's Article 8 rights if it is **necessary and proportionate** for these activities to take place. RIPA first requires that the person granting an authorisation to believe that the authorisation is necessary for the purpose of preventing and detecting crime or of preventing disorder; therefore there is a requirement that applicants and Authorising Officers consider why the use of covert surveillance is necessary in the specific investigation and what it will achieve.

2.5.2 If the activities are necessary, the person granting the authorisation must believe that they 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 the operational terms. Both the officer making the application and the Authorising Officer should consider the following test when deciding that the proposed covert surveillance is proportionate:

a) Is the proposed covert surveillance proportionate to the mischief under investigation;

b) Is the proposed covert surveillance proportionate to the degree of anticipated intrusion on the target and others; and

c) Is the proposed covert surveillance the only option and have other overt means been considered and discounted.

2.5.3 The activity will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means. For example it may be acceptable in a benefit "living together" case for surveillance over seven days but not extended over three months. All such activity should be carefully managed to meet the objective in question and must not be arbitrary or unfair.

2.6 Collateral Intrusion

2.6.1 Before authorising surveillance the Authorising Officer should 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). Measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the lives of those not directly connected with the investigation or operation.

2.6.2 An application for an authorisation should include an assessment of the risk of any collateral intrusion. The Authorising Officer should take this into account, when considering the proportionality of the surveillance.

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

2.6.4 Any person granting or applying for an authorisation will also need to be aware of particular sensitivities in the local community where the surveillance is taking place and of similar activities being undertaken by other public authorities which could impact on the deployment of surveillance.

2.7 Central Record of Authorisations

2.7.1 A central retrievable record of all authorisations is required to be kept by the Council and regularly updated. Whenever an authorisation is granted, renewed or cancelled the original signed document must be passed to the Co-ordinating Officer who maintain's the Central Record of Authorisations. On receipt of the documentation the required information will be recorded in the central register.

2.7.2 The record is required to be made available to the relevant Commissioner or an Inspector from the Investigatory Powers Comissioner's Office, upon request.

2.7.3 These records should be retained for a period of five years from the ending of the authorisation and should contain the following information:

- the unique reference number (URN) – this will be provided by the Co-ordinating Officer when requested by the officer applying for the authorisation;
- the type of authorisation; (SBC officers can only conduct directed surveillance)
- the date the authorisation was given;
- the name of the Authorising Officer;
- the title of the investigation or operation, including a brief description and names of subjects, if known;
- the date for review;
- the date review was undertaken;
- if the authorisation is renewed, when it was renewed and who authorised the renewal, including the name of the Authorising Officer;
- whether the investigation is likely to result in obtaining confidential information; and
- the date the authorisation was cancelled.

2.7.4 In all cases, the officer responsible for the investigation (Investigation Manager) must maintain the following documentation which need not form part of the central retrievable record:

- copy of the application and a copy of the authorisation together with any supplementary documentation and notification of the approval given by the Authorising Officer;
- copy of any renewal of any authorisation together with supporting documents
- any authorisation which was granted or renewed orally (an urgent case) and the reason why the case was considered urgent
- record of the period over which the surveillance has taken place;
- any risk assessment raised in relation to a CHIS;
- the circumstances in which tasks were given to the CHIS;
- the value of the CHIS to the investigation;
- the frequency of reviews prescribed by the Authorising Officer, recommended monthly;
- record of the result of each review of the authorisation;
- copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested; and
- date and time when any instruction were given by the Authorising Officer since using CHIS.

2.8 **Retention and Destruction**

2.8.1 Where the product of surveillance could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with established disclosure requirements for a suitable further period, commensurate to any subsequent review.

2.8.2 There is nothing which prevents material obtained from properly authorised surveillance from being used in other investigations. Authorising Officers must ensure compliance with the appropriate data protection requirements and that arrangements for the handling, storage and destruction of material obtained through the use of covert surveillance are followed.

2.8.3 Investigating officers are expected to keep accurate and full records of investigations. All notebooks (including QB50 for relevant Officers), surveillance logs and other ancillary documentation that relate to surveillance must be maintained for five years and available for management or regulatory inspection on demand.

3. SPECIAL RULES ON AUTHORISATIONS

(Directed Surveillance and CHIS)

3.1 Care should be taken in cases where the subject of the investigation or operation might reasonably expect a high degree of privacy eg, where confidential information is involved. Confidential information consists of matters subject to legal privilege, confidential personal information or confidential journalistic material. For example, extra care should be given where, through the use of surveillance, it would be possible to acquire knowledge of discussions between a minister of religion and an individual relating to the latter's spiritual welfare, or where matters of medical or journalistic confidentiality or legal privilege may be involved.

3.2 In cases where through the use of surveillance it is likely that knowledge of confidential information will be acquired, the use of surveillance is subject to a higher level of authorisation, and must be authorised by the Chief Executive (who is designated the RIPA Senior Responsible Officer) or in their absence the deputy SRO.

3.3 Where a juvenile or vulnerable person is to be used as a CHIS the Investigating Officer must, when seeking an authorisation:

(a) make a risk assessment to demonstrate that the physical and psychological risks have been identified, evaluated and explained to the CHIS, and

(b) that an appropriate adult will be present at meetings of any CHIS under the age of 18.

3.4 Where the authorisation is for the employment of a juvenile or vulnerable CHIS the authorisation **must** be obtained by the Chief Executive (who is designated the RIPA Senior Reponsible Officer) or in their absence, the deputy SRO.

4. AUTHORISATION PROCEDURE FOR COVERT SURVEILLANCE

(Directed Surveillance and CHIS)

The appropriate RIPA forms are available from the Intranet, under Service Units; Legal; Shared Documents; Guidance, RIPA; Covert Surveillance Forms and Code of Practice.

Application Forms:

- Application for the use of Directed Surveillance form
- Application for the use of CHIS form
- Judicial Application / Order form

4.1 Before covert surveillance can be conducted, an application for the use of directed surveillance form and/or an application for the use of CHIS form must be completed and authorised in writing by the Authorising Officer.

4.2 Local Authorites cannot rely on the provision for urgent authorisation being given orally by the Authorising Officer as there is the requirement of obtaining judicial approval.

There are however guidelines for obtaining urgent judicial approval and these are detailed below at paragraph 4.15. It should be remembered that no RIPA authority is required in situations where surveillance is an immediate response to events i.e. where criminal activity is observed during routine duties and officers conceal themselves to observe what is happening.

4.3 The application should include:

- the reason why the authorisation is necessary i.e. for the purpose of preventing and detecting crime or of preventing disorder *(this is the only permitted ground open to Local Authorities)*
- an adequate explanation of the reason why the surveillance is considered proportionate to what it seeks to achieve;
- the nature of the surveillance including what surveillance equipment is to be used (the operation must be spelt out in sufficient detail on the application form for the Authorising Officer to have a clear idea of exactly what they are being asked to authorise);
- a map showing where the surveillance will take place;
- details of other methods considered and why they were deemed not to be appropriate;
- the identities, where known, of those to be the subject of the surveillance;
- an explanation of the information desired from the surveillance;
- the details of any potential collateral intrusion and why the intrusion is justified;
- the details of any confidential information that is likely to be obtained as a consequence of the surveillance;
- the level of authority required (or recommended where that is different) for the surveillance; and
- a subsequent record of whether authority was given or refused, by whom and the time and date.

Good Practice Tips:

- ensure all questions are answered properly and appropriate boxes ticked;
- prior to submitting the application review the case file and discuss the case with the Authorising Officer to tease out additional information required and to fill any gaps, provide adequate information on the application form for it to stand alone;
- Information must be clear and unambiguous;
- set out in full and explain any acryomns; and
- explain operational processes which may otherwise require service specific knowledge.

4.4 To enable application forms for directed surveillance to be completed with sufficient detail drive bys are permitted to identify whether a location is suitable for surveillance. However, the practice should not be abused and repeated and/or systematic use of drive bys may require application for surveillance forms to be completed and authorisation granted by an Authorising Officer. If surveillance is to commence immediately authorisation **must** be sought first.

Authorisation:

4.5 Responsibility for authorising the carrying out of covert surveillance rests with the Authorising Officer and requires the personal authority of the Authorising Officer. **In no circumstances should an officer authorise until they have met the training standard stipulated by the Senior Responsible Officer.**

4.6 Authorising Officers must insist on the operation being described in sufficient detail *on the application form* for them to have a clear idea of exactly what they are being asked to authorise and so that they have a sufficient *aide-memoir* to be able to withstand cross-examination in Court, maybe after a lapse of some years. The application form must stand alone in supporting the authorisation. Only what is written on the form would be used in Court to justify authorisation of surveillance being granted, therefore Authorising Officers must clearly describe exactly what activities they are authorising.

4.7 An authorisation can only be granted by the authorising officer where they believe that the use of covert surveillance is **necessary** in the investigation for the purposes of preventing and detecting crime or of preventing disorder and that the surveillance is **proportionate** to what it seeks to achieve, i.e it satisfies the test set out at 2.5 above.

4.8 In completing their authorisation the Authorising Officer should include a statement detailing their reasons for considering that application is necessary and proportionate incorporating the 5 "W's"; these being: "who", "what", "where", "when", "why" and "how".

4.9 In addition, when an authorisation is sought for the use of CHIS, the Authorising Officer must be satisfied that:

(a) that there will at all times be a person holding an office, rank or position with the relevant investigating authority who will have day-to-day responsibility for dealing with the source on behalf of that authority, and for the source's security and welfare;

(b) that there will at all times be another person holding an office, rank or position with the relevant investigating authority who will have general oversight of the use made of the source;

(c) that there will at all times be a person holding an office, rank or position with the relevant investigating authority who will have responsibility for maintaining a record of the use made of the source;

(d) that the records relating to the source that are maintained by the relevant investigating authority will always contain particulars of all such matters (if any) as may be specified for the purposes of this paragraph in regulations made by the Secretary of State;

(e) that records maintained by the relevant investigating authority that disclose the identity of the source 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; and

(f) that a risk assessment has been carried out to determine the risk to the source of any tasking and the likely consequences should the role of the source become known. The ongoing security and welfare of the source, after the cancellation of the authorisation, should have also been considered at this stage.

For further information please refer to paragraphs 1.22 to 1.29 above.

4.10 Authorising Officers should, where possible, complete their authorisation by hand to avoid being challenged at a later date as to the authenticity of their authorisation.

4.11 Where a previously unidentified subject is identified or an additional subject is subsequently identified during the course of surveillance, the surveillance may continue in order to maintain contact. Thereafter, a revised authorisation will be required to cover the additional subject etc. New individuals **must not** be added to the original authorisation retrospectively.

Judicial Approval:

4.12 As soon as an authorisation has been granted through the internal procedure the following steps must be taken to obtain judicial approval:

1. HMCTS administration at the magistrates' court should be contacted by calling 01622 671041 for a hearing to be arranged – such hearings will be held in private.
2. A copy of the original RIPA authorisation and supporting documentation should be provided to the Magistrate and **should contain all information that is relied upon**. The authorisation can be considered by a single lay Magistrate (sometimes refererred to as a Justice of the Peace) supported by a Legal Advisor to the Court or a District Judge.
3. Two copies of the partially completed judicial approval/order form should be provided to the Magistrate – one for the Court to keep and one for the Council.
4. Attend hearing.

Any officer that attends on behalf of the Council must be authorised to do so by the Head of Legal under section 223 of the Local Government Act 1972.

4.13 Consideration should be given as to who is the most appropriate person to attend the hearing to request judicial approval. As it is likely that the Magistrate will have questions for whoever attends it should be someone with a detailed knowledge of the case. It may be that the most appropriate person to attend is the Authorising Officer as only they can explain their reasoning on necessity, proportionality, collateral intrusion and risk. It is recognised that this is not always practicable, and in these cases it is likely that the investigating officer should attend and promptly report back any comments made by the Magistrate to the Authorising Officer.

*NB: All evidence of necessity and proportionality **must** be in the RIPA/CHIS application form as it is not sufficient to provide oral evidence at the hearing where this is not reflected or supported in the papers provided.*

4.14 Following consideration of the case the Magistrate will complete the order section of the judicial application / order form recording their decision to either approve or refuse the authorisation or to refuse and quash the original authorisation.

4.15 Whilst Home Office Guidance urges Local Authorities to make local arrangements to deal with out of hours access to a Magistrate for urgent cases our local HMCTS legal staff have advised that they do not envisage there to ever be a need for the authority to require urgent access, therefore all applications should be made in Court hours. The Senior Responsible Officer will continue to review the situation and if it is proven

that there is a need for local arrangements for urgent cases to be made we will contact the Court again.

NB: It should be remembered that in most emergency situations it is likely that the police would have the power to act, and in such cases they would be able to authorise the activity without prior judicial approval.

4.16 Authorising Officers should not be responsible for authorising investigations or operations in which they are directly involved, although it is recognised that this may sometimes be unavoidable, especially in the case of small organisations, or where it is necessary to act urgently

Directed surveillance conducted from premises
(ref: R v Kenneth Johnson)

4.17 In the event that covert surveillance is required to be conducted from premises the following guidelines must be followed:

- Prior to covert surveillance being conducted from premises the line manager (or above) responsible for the investigation must visit the premises to ascertain the attitude of the occupiers to the surveillance activities and to the possible disclosure of information which might enable them to be identified.

- Immediately before trial the Head of Services (or above) must ascertain whether the occupiers of the premises are the same as when the surveillance took place and, whether they are or not, what their feelings are as to the disclosure of information which might cause them to be identified.

Reviews:

Forms:
- Review of the use of Directed Surveillance form
- Review of the use of CHIS form

4.18 Written authorisations granted under RIPA for a CHIS cease to have effect twelve months after the date of granting of the authorisation. All other written authorisations under RIPA cease to have effect three months after the authorisation was granted.

4.19 Reviews of authorisations should be undertaken by the officer responsible for conducting the investigation (Investigation Manager), and approved by the Authorising Officer, to assess the need for the surveillance to continue. Reviews should take place at least monthly and immediately after the date the surveillance is due to end. The Authorising Officer may review the authorisation on a more frequent basis where it is considered necessary and practicable for example where the surveillance provides access to confidential information or involves collateral intrusion.*There is no requirement for the JP to consider internal reviews.* A copy of the review form should be retained by the officer responsible for conducting the investigation (Investigation Manager) and the original should be passed to the RIPA Co-ordinating Officer.

Renewals:

Forms:
- Renewal of Directed Surveillance form
- Renewal of CHIS form

4.20 If at any time before an authorisation would cease to have effect, the Authorising Officer considers it necessary for the authorisation to continue for the purpose for which it was given, they may renew it in writing for a further period of **three months** for directed surveillance and **twelve months** for a CHIS.

4.21 A renewal takes effect at the time at which, or day on which the authorisation would have ceased to have effect but for the renewal. An application for renewal should not be made until shortly before the authorisation period is drawing to an end. Any person who would be entitled to grant a new authorisation can renew an authorisation.

4.22 Applications for renewal of an authorisation for covert surveillance should record:

- whether this is the first renewal or every occasion on which the authorisation has been renewed previously;
- any significant changes to the information at paragraph 4.3;
- the reasons why it is necessary to continue with the directed surveillance;
- the content and value to the investigation or operation of the information so far obtained by the surveillance; and
- the result of regular reviews of the investigation or operation.

4.23 Authorisations may be renewed more than once, provided they continue to meet the criteria for authorisations. A copy of the renewal forms should be retained by the officer responsible for conducting the investigation (Investigation Manager) and the original should be passed to the RIPA Co-ordinating Officer for the required information to be recorded in the Central Record of Authorisations (see paragraph 2.7).

4.24 **Following the internal authorisation for renewal process it will again be necessary to obtain judicial approval for the authorisation to be renewed and the same process detailed in 4.12 to 4.14 above should be followed.**

NB: Where renewals are timetabled to fall outside of court hours it is for the investigating officer on behalf of the Local Authority to ensure that the renewal is completed ahead of the deadline.

Cancellations:

Forms:

- Cancellation of Directed Surveillance form
- Cancellation of CHIS form

4.25 A written authorisation granted by an Authorising Officer will cease to have effect (unless renewed) at the end of a period of **three months in relation to Directed Surveillance** or **twelve months in relation to CHIS** beginning with the day on which it took effect, however the Authorising Officer who granted or last renewed the authorisation must promptly cancel the authorisation if he is satisfied that the covert surveillance no longer meets the criteria for authorisation, including, but not limited to, where during the investigation it becomes clear that the offence being investigated no longer meets the crime threshold.

4.26 As soon as the decision is taken that covert surveillance should be discontinued, the instruction must be given to those involved to stop all surveillance of the subject(s) and a record made of the date and time when the instruction was given. A cancellation of

the use of directed surveillance form must be completed by the officer responsible for conducting the investigation (Investigation Manager) and signed by the Authorising Officer. *There is no requirement for the Magistrate to consider cancellations.*

4.27 Cancellation forms should be retained by the Investigating Manager and the original should be passed to the RIPA Co-ordinating Officer for the required information to be recorded in the Central Record of Authorisations (see paragraph 2.7).

To ensure prompt cancellation Investigation Managers should advise the Authorising Officer as soon as surveillance activity has ceased.

5. AUTHORISATION PROCEDURES FOR COMMUNICATIONS DATA

5.1 Only officers authorised by the Council's Designated Person can submit applications via the NAFN secure website facility. Authorised officers are assigned a website username and password to access the NAFN SPoC application system.

5.2 Applications should detail the necessity,purpose and proportionality of each request for information, in addition to consideration of collateral intrusion arising from the request for information. The level of detail should be as required for covert surveillance and CHIS applications – See 4.3.

5.3 Applications which do not provide adequate detail will be returned to applying officers for reworking prior to submission to the Council's Designated Person (DP) for consideration and approval. Applications will only be approved where the DP considers the application to be necessary and proportionate to the investigation.

5.4 As soon as an authorisation has been granted through the internal procedure it will be for the Council to obtain judicial approval following the procedure detailed above at paragraphs 4.12 to 4.14. The Magistrate will complete the order section of the judicial application / order form reflecting their decision after which the Council will then be required to upload a copy of this order to the NAFN SPoC system.

6. Authorisation Control Matrix/ Aide-memoire:

6.1 To assist officers responsible for conducting investigations (Investigation Managers) to maintain appropriate records and comply fully with the Regulations a suitable Authorisation Control Matrix has been included at Appendix C. Dates of Reviews and when Authorisations cease should also be diarised as a further aid-memoire so that Reviews, Renewals and Cancellations are properly completed in a timely manner.

7. Complaints Relating to the use of RIPA

7.1 The Investigatory Powers Tribunal is a court which investigates and determines complaints which allege that public authorities or law enforcement agencies have unlawfully used covert techniques and infringed an individuals right to privacy, as well as claims against the security and intelligence agencies for conduct which breaches a wider range of our human rights. Where a member of the public wishes to complain about the Council's use of, or conduct of these powers they should be directed towards the Tibunal's website at http://www.ipt-uk.com/.

8. Non-RIPA Surveillance

Where the crime threshold for surveillance cannot be met, surveillance can still be considered as a last resort if it is deemed to be both necessary and proportionate. In such cases the same internal procedure used for the authorisation, renewal, review and cancellation of a RIPA application set out on pages 15 to 19 are to be followed, however the relevant non-RIPA form is to be used with all documentation being held centrally by the RIPA Co-ordinating Officer. For non RIPA applications there is no requirement to obtain Judicial Approval however all internal procedures must be followed to record the non-RIPA activity.

Appendix A

Relevant Legislation and Guidance

The Data Protection Act 2018

The Act provides six principles to be observed to ensure that the requirements are complied with. They provide that personal data (which includes personal data obtained from **covert surveillance techniques)** must:

1 be used fairly, lawfully and transparently;
2 be used for specified, explicit purposes;
3 be used in a way that is adequate, relevant and limited to only what is necessary;
4 be accurate and, where necessary, kept up to date;
5 be kept for no longer than is necessary; and
6 be handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage.

The Human Rights Act 1998

Article 8 of the European Convention on Human Rights is relevant in the context of **covert surveillance** in that it states:

- everyone has the right to respect for his private and family life, home and correspondence;

- there is to be no interference with the exercise of these rights by the local authority, except where such interference is in accordance with the law and is necessary in a democratic society in the interest of national security, public safety or the economic well being 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

Article 6 of the Convention is also relevant in the context of **covert surveillance** in that everyone has the right to a fair trial, including internal procedures or hearings, and fairness extends to the way in which evidence is obtained.

The Regulation of Investigatory Powers Act 2000

- The Act strikes a balance between community responsibilities, including effective law enforcement and individual rights and freedoms. The principles of RIPA are as follows:

- Surveillance is an intrusion into the privacy of the citizen. It should not be undertaken unless it is necessary, proportionate to the alleged offence and properly authorised. Where there is an alternative legal means of obtaining information that is less intrusive on the rights of the citizen, the alternative course rather than surveillance should be taken.

- Surveillance will be conducted within the constraints of the Council. It will cease when evidence sought has been obtained or when it becomes clear that the evidence is not going to be obtained by further surveillance. At that point authorisation must be cancelled.

- In every instance where surveillance is authorised the officer who conducts surveillance will consider and make plans to reduce the level of collateral intrusion into the privacy of third parties.

- All outstanding surveillance authorisations will be reviewed at regular intervals and cancelled where there is no further need for surveillance.

- All officers involved in applying for, authorising or undertaking surveillance will understand the legal requirements set out in RIPA and the Code of Practice. They will personally take responsibility of their involvement.

- All authorisations, notebooks, surveillance logs and other ancillary documentation that relates to surveillance will be maintained to the required standard for three years. All documentation will be volunteered for any management or regulatory inspection on demand.

- Any failure of any part of the process will be brought to the attention of the manager responsible for the investigation.

- Wilful disregard of any part of the Surveillance Code of Practice or of internal procedures will be dealt with in line with Council policy.

Protection of Freedoms Act 2012

The Act amended the Regulaton of Investigatory Powers Act 2000 (RIPA) to make local authority authorisation subject to judicial approval. It also limited a Local Authority's use of RIPA so that authorisations could only be obtained for directed surveillance to prevent or detect criminal offences that are either punishable, whether on summary conviction or indictment, by a minimum term of at least six months imprisonment or are related to the underage sale of alcohol and tobacco.

Investigatory Powers Act 2016

The Act will provide a new framework to govern the use and oversight of investigatory powers by law enforcement and the security and intelligence agencies. The aim of the Act is to bring together all of the powers already available to law enforcement and the security and intelligence agencies to obtain communications and data about communications and will make these powers and the safeguards that apply to them clear and understandable. In addition it creates a powerful new Investigatory Powers Commissioner to oversee how these powers are used and ensures powers are fit for the digital age.

Criminal Procedures & Investigation Act 1996 (CPIA)

The Act sets out legal obligations concerning criminal investigations. The principles of the Act are as follows:-

- **Record** - Information must be recorded in a durable and retrievable form. It must be full & factual. File notes must be contemporaneous, dated & preferably timed. There should be no personal comments, biased opinions, and prejudiced observations.

- **Retain** - All material obtained in the course of an investigation must be retained in the investigation file. The origin, date & if appropriate the time it was obtained must be recorded. The reasons for action must be recorded, including any request for authorised surveillance, and details of the risk assessment.

- **Reveal** - 3 clearly identifiable roles on all investigation files:-
    - Investigator
    - Officer in Charge of the Investigation
    - Disclosure Officer

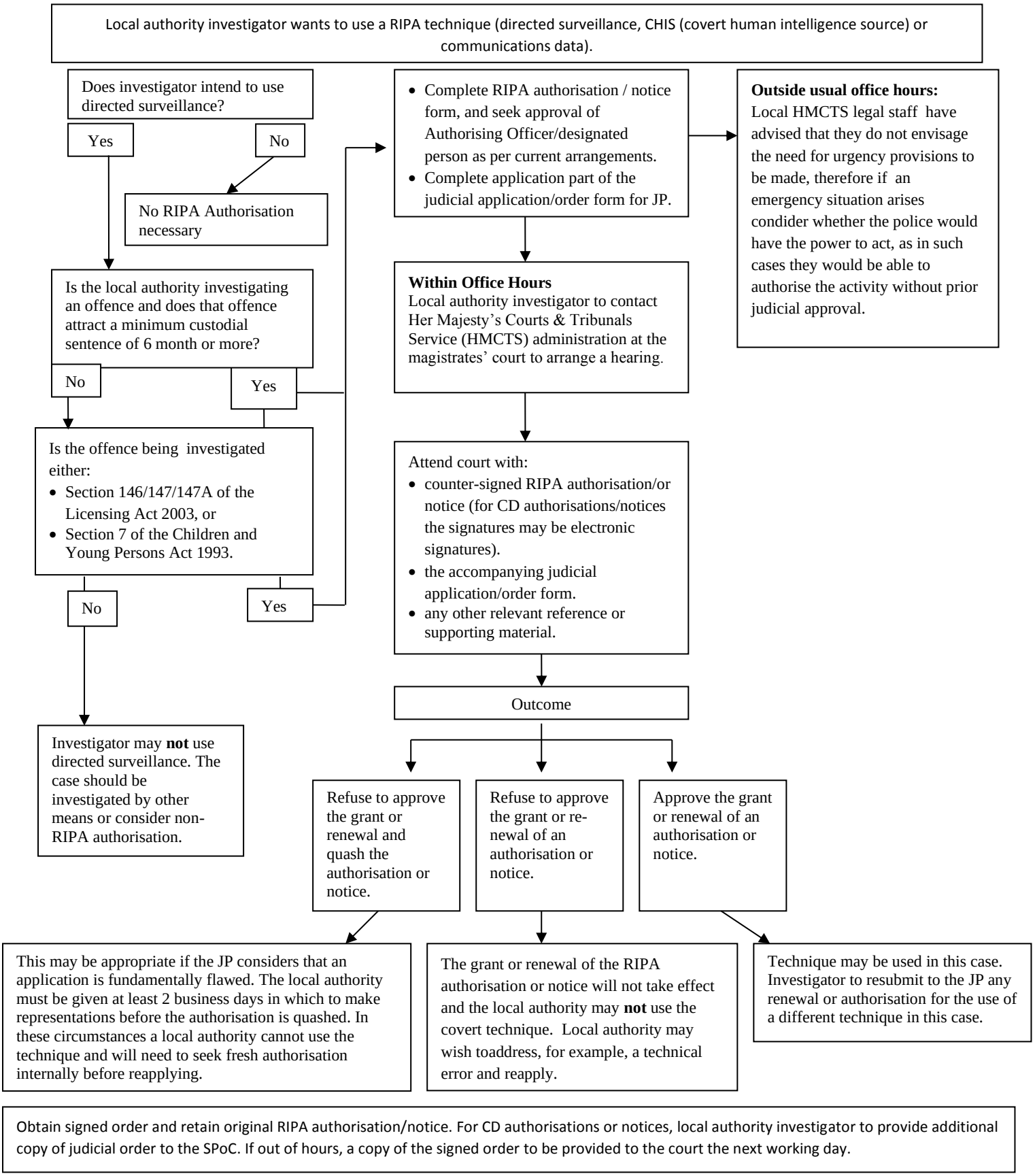
  Unused material is listed on two schedules: -
    - Non-sensitive
    - Sensitive.

Guidance Notes and Codes of Practice:

- Covert Surveillance and Property Interference Code of Practice – Home Office https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/384975/Covert_Surveillance_Property_Interrefernce_web__2_.pdf
- Covert Human Intelligent Source Code of Practice – Home Office https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1123687/Revised_CHIS_Code_of_Practice_December_2022_FINAL.pdf
- Acquisition and Disclosure of Communications Data Code of Practice – Home Office https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/426248/Acquisition_and_Disclosure_of_Communications_Data_Code_of_Practice_March_2015.pdf
- Guidance to local authorities in England and Wales on the judicial approval process for RIPA and the crime threshold for directed surveillance – Home Office, October 2012 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/118173/local-authority-england-wales.pdf

Information can also be obtained from the website of the Investigatory Powers Commissioner's Office at https://www.ipco.org.uk/ who has obsorbed the powers of the Office of Surveillance Commissioners and the Interception of Communications Commissioner's Office.

LOCAL AUTHORITY PROCEDURE: APPLICATION TO A JUSTICE OF THE PEACE SEEKING AN ORDER TO APPROVE THE GRANT OF A RIPA AUTHORISATION OR NOTICE



Appendix C

AUTHORISATION CONTROL MATRIX							
OP/INVESTIGATION NAME:				**UNIQUE REFERENCE NUMBER:**			
SUBJECT NO.	**APPLICATION**	**AUTHORISATION**		**RENEW**	**REVIEW**	**CAN-CELLED**	**EXPIRY DATE**
		ORAL	**WRITTEN**				